NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

BEYOND LINE OF SIGHT (BLOS) COMMAND AND CONTROL (C2) CAPABILITY TO IMPROVE DISASTER RESPONSE AND RECOVERY

by

Robert H. Schulz Jr.

September 2013

Thesis Advisor: James C. Moltz
Second Reader: Joseph Utschig

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704–0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202–4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704–0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2013	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE BEYOND LINE OF SIGHT (BLOS) COMMAND AND CONTROL (C2) CAPABILITY TO IMPROVE DISASTER RESPONSE AND RECOVERY		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Robert H. Schulz Jr.			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943–5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE** A	

13. ABSTRACT (maximum 200 words)

The ability to manage and monitor assets provides undeniable benefits in accomplishing mission objectives. The value of these capabilities is exponentially greater in disaster situations. This thesis introduces the BLOS C2 capability as a method of improving disaster response and recovery by enhancing situational awareness (SA) as well as command and control (C2). Demonstrated overseas in support of U.S. military battlespace coordination, the BLOS C2 capability promotes seamless communication and data sharing by means of sensor data and a truly common operational picture. Using the proven model that has improved mission effectiveness for the U.S. military, this thesis uses the Department of Homeland Security (DHS) and other levels of government involved in emergency response as case studies for analyzing the BLOS C2 capability in an effort to fill gaps in interoperability and information sharing. After analyzing each of these case studies, the application of the BLOS C2 capability will be considered and evaluated for potential benefits. Once these evaluations are made, recommendations will be offered that are aimed at implementing the BLOS C2 capability at all levels of government. These recommendations will provide DHS with courses of action that could enhance SA and C2, and potentially improve response and recovery efforts in the event of a disaster.

14. SUBJECT TERMS Common Operational Picture, Situational Awareness, Command and Control, Homeland Security, Network Architecture, Intelligence, Surveillance, Information Technology, Public Service, Information Sharing, Interoperability	**15. NUMBER OF PAGES** 89
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540–01–280–5500 Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

BEYOND LINE OF SIGHT (BLOS) COMMAND AND CONTROL (C2) CAPABILITY TO IMPROVE DISASTER RESPONSE AND RECOVERY

Robert H. Schulz Jr.
Civilian, United States Navy
B.A., University of California, 2010

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND DEFENSE AND SECURITY)**

from the

**NAVAL POSTGRADUATE SCHOOL
September 2013**

Author: Robert H. Schulz Jr.

Approved by: James C. Moltz
Thesis Advisor

Joseph Utschig
Second Reader

Mohammad Hafez
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The ability to manage and monitor assets provides undeniable benefits in accomplishing mission objectives. The value of these capabilities is exponentially greater in disaster situations. This thesis introduces the BLOS C2 capability as a method of improving disaster response and recovery by enhancing situational awareness (SA) as well as command and control (C2). Demonstrated overseas in support of U.S. military battlespace coordination, the BLOS C2 capability promotes seamless communication and data sharing by means of sensor data and a truly common operational picture. Using the proven model that has improved mission effectiveness for the U.S. military, this thesis uses the Department of Homeland Security (DHS) and other levels of government involved in emergency response as case studies for analyzing the BLOS C2 capability in an effort to fill gaps in interoperability and information sharing. After analyzing each of these case studies, the application of the BLOS C2 capability will be considered and evaluated for potential benefits. Once these evaluations are made, recommendations will be offered that are aimed at implementing the BLOS C2 capability at all levels of government. These recommendations will provide DHS with courses of action that could enhance SA and C2, and potentially improve response and recovery efforts in the event of a disaster.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AIS	Automatic Identification System
ATT	Architecture and Advanced Technology
AVL	Automated Vehicle Locations
BAO	Battlefield Air Operations
BLOS	Beyond Line of Sight
BLOS C2	Beyond Line of Sight Command and Control
C2	Command and Control
C4ISR	Command, Control, Communications and Computers, ISR
CAL FIRE	California Department of Forestry and Fire Protection
CBP	Customs and Border Protection
CCTV	Closed Circuit Television
COP	Common Operational Picture
CoT	Cursor on Target
DHS	Department of Homeland Security
DOD	Department of Defense
DOJ	Department of Justice
ECC	Emergency Command Center
ECPC	Emergency Communications Preparedness Center
EMP	Electromagnetic Pulse
EMS	Emergency Medical Service
EO	Executive Order
EO/IR	Electro-Optical/Infrared
FAA	Federal Aviation Authority
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
FirstNet	First Responders Network Authority
FMV	Full Motion Video
GETS	Government Emergency Telecommunications Services
GJXDM	Global Justice XML Data Model

GPS	Global Positioning Satellite
HAM	Amateur Radio
ICGS	Integrated Coast Guard Systems
ICS	Incident Command System
IP	Internet Protocol
ISR	Intelligence, Surveillance, and/or Reconnaissance
ITAP	Interoperable Communications Technical Assistance Program
JBAIIC	Joint Battlespace Awareness ISR Integration Capability
LEO	Low Earth Orbit
LMR	Land Mobile Radio
LOS	Line of Sight
LRIT	Long Range Identification Tracking
MCC	Mobile Communication Center
MCV	Mobile Command Vehicle
MDA	Maritime Domain Awareness
MDT	Mobile Data Terminal
MERS	Mobile Emergency Response Support
MF/HF	Medium Frequency/ High Frequency
MHz	Megahertz
MTS	Marine Transportation System
NAIS	Nationwide Automatic Identification System
NCS	National Communications System
NECP	National Emergency Communications Plan
NGEN	Next Generation
NGN-PS	Next Generation Network Priority Service
NIEM	National Information Exchange Model
NPS	Naval Postgraduate School
NPSBN	Nationwide Public Safety Broadband Network
NS/EP	National Security and Emergency Preparedness
NTIA	National Telecommunications and Information Administration
OCONUS	Outside of the Continental United States
OEC	Office of Emergency Communications

P25	Project 25
P25IP	Project 25 with Internet Protocol
PPLI	Precise Position and Location Information
PWCS	Ports, Waterways, and Coastal Security
RFP	Request for Proposal
SA	Situational Awareness
SCIP	Statewide Interoperability Plans
SPD	Salinas Police Department
SPoI	Sensor Point of Interest
SWIC	Statewide Interoperability Coordinators
TSP	Telecommunications Service Priority
UAV	Unmanned Aerial Vehicle
UHF	Ultra-High Frequency
USCG	United States Coast Guard
VHF	Very High Frequency
VoIP	Voice over Internet Protocol
WPS	Wireless Priority Services

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

First and foremost, I would like to thank God for the wisdom and perseverance that He has bestowed upon me during this thesis project, and for providing me with the opportunity to pursue a higher education.

Second, I would like to thank my family for all their love and encouragement. For my mother and the memory of my father, who have provided a loving home and continually support me in all my pursuits. My brother, best friend and role model, David, for inspiring me to succeed through the exceptional examples he sets. For my aunt, uncle, and cousins, Nick and Mara, who constantly remind me of the importance of family.

Next, my thanks to my advisors who provided intellectual stimulation and guidance throughout the writing process of this thesis. To Professor Clay Moltz, who despite my chaotic schedule maintained his support and willingness to help. To Joe Utschig, who has mentored me in every possible way, and whom I hope to emulate as a leader one day.

Additionally, this thesis would not have been possible without the Distributed Information Systems Experimentation (DISE) group at the Naval Postgraduate School. The DISE group has given me the opportunity to research topics and technologies that impact our nation's efforts in securing the homeland.

I would also like to express my deepest gratitude to the men and women who have served in the U.S. Armed Forces, who make countless sacrifices in ensuring our Nation's freedom.

Last, but not least, I would like to thank my beautiful fiancé, Laura, for being my most enthusiastic cheerleader and always providing me with unconditional love and support. I look forward to spending the rest of our lives together.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. MAJOR RESEARCH QUESTION

Since the release of the 9/11 Commission report, the Department of Homeland Security (DHS) has made strides toward the implementation of a nationwide interoperable communications network. In doing so, DHS has focused on ensuring optimal communications capabilities for the nation's emergency responders, both in the private sector and at every level of government. As the Nationwide Public Safety Broadband Network (NPSBN) initiative takes off, the active participation of local and state first responder organizations is imperative in successfully deploying an entirely interoperable network for effective disaster response and recovery.

The Joint Battlespace Awareness ISR Integration Capability (JBAIIC), a field experimentation initiative at the Naval Postgraduate School (NPS), specializes in ensuring that Intelligence, Surveillance, and/or Reconnaissance (ISR) data is immediately available to coalition warfighters to meet mission demands. A wide variety of aerial and terrestrial systems are used to acquire and publish ISR data, from hand-held devices to unmanned aerial vehicles (UAV) and satellites. Through the exploitation of ISR data, such as global positioning system (GPS) and full motion video (FMV), over a tactical wireless network, JBAIIC can offer enhanced situational awareness (SA) to decision makers as well as ground units to improve command and control (C2). Currently, JBAIIC is involved in deploying a Beyond Line Of Sight (BLOS) C2 capability for use in the battlefield in order to support a battlespace coordination advantage and improved mission fulfillment. In achieving this benefit, the BLOS C2 capability promotes seamless communication and data sharing by means of sensor data and a common operational picture (COP).

Given the nationwide communications interoperability initiative that DHS is emphasizing and JBAIIC's BLOS C2 expertise, the following research question is raised: Could a Beyond Line Of Sight Command and Control capability improve disaster response and recovery efforts at the federal, state, and local levels?

B. IMPORTANCE

National Emergency Medical Service (EMS) personnel and first responders at all levels must have access to reliable and seamless communications in order to effectively coordinate response and recovery operations in the event of a disaster. Agencies across the U.S. have learned the harsh consequences in failing to establish relationships with outside organizations. Events such as the attacks on 9/11 and Hurricane Katrina serve as permanent reminders of these very failures. In successfully deploying the DHS-led interoperable communications network, integration across first responder organizations can theoretically improve the effectiveness of disaster response and recovery. In leveraging this initiative, the BLOS C2 capability can contribute to the exploitation of relevant SA data through a COP, helping to achieve an enhanced coordination among disaster relief efforts. When major emergencies require the aid of federal, state, and local organizations, this capability has the potential to aid in the delivery of key resources to the right place in a timely manner. The unpredictable nature of disasters has a tendency to paralyze the most critical infrastructures at the worst possible time. In a scenario where communications represent the lifelines of victims requiring time-sensitive attention, the network for carrying out effective disaster response must be resilient and interoperable. Once this capability is accomplished, BLOS C2 sensor data such as aerial-provided FMV and GPS locating could be shared across the response network. The COP could then serve as an interactive community map, allowing users to share relevant information about impact areas to respond accordingly. Additionally, with LOS to aerial assets carrying radio repeaters, the range of the interoperable emergency communications architecture could be extended to support a larger impact area, or a ground LOS-denied environment. Due to the potential of benefits offered by the BLOS C2 capability, its integration into the nationwide interoperability effort currently being assessed by DHS may facilitate enhanced communications and information sharing. When local and state organizations begin to comply with the national communications interoperability standard, the SA gained through the BLOS C2 capability could significantly improve the DHS coordination of cross-agency support of disaster response and recovery.

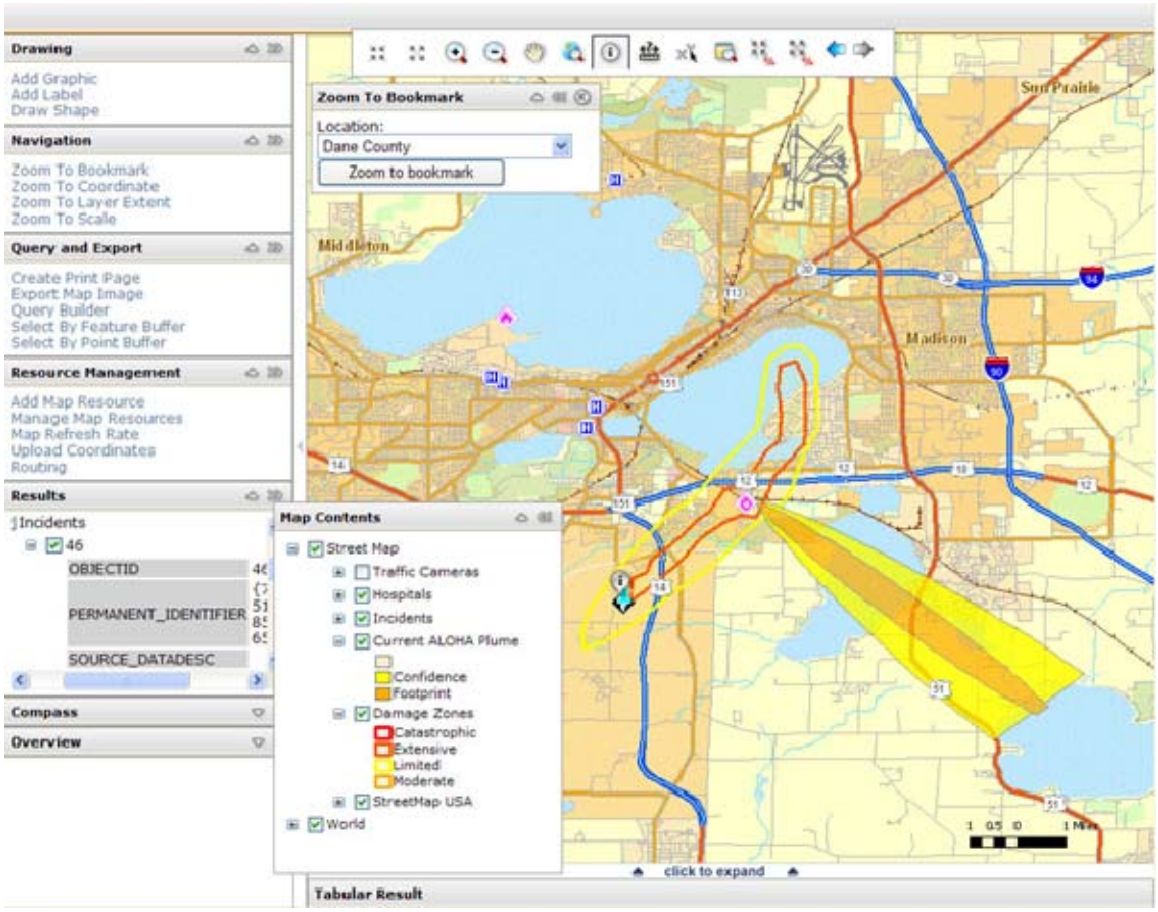

Figure 1. Example of a Common Operational Picture. (From ESRI Technologies, n.d.)

C. PROBLEMS AND HYPOTHESES

Problematic areas raised by the major research question include the financial and cultural hurdles involved in the implementation of new communications systems. In delivering a nationwide standardization requirement for interoperable radio systems, cash-strapped local organizations that rely on larger county communications infrastructure could be stranded from the transitioning cooperative efforts, posing unforeseeable complications. The financial constraints of underfunded public safety agencies could be further aggravated once the majority of agencies have switched over. While participating agencies will benefit in the proportional sharing of the new communications infrastructure costs, this potentially leaves non-participants with the financial burdens of independently managing their own radio communications systems.

Non-participation in the interoperable radio system may also be due to cultural stubbornness and policy restrictions. What may potentially be found is that organizations grounded in traditional operational habits may deny the shift toward technological advancements. Additionally, since the implementation of a new communications infrastructure requires the backing of multiple members of a jurisdiction, policy implementation may encounter differing opinions on relevance and prioritization in the best interest of a given community. Familiarization of a new communications system as well as the BLOS C2 system may require additional funding for training purposes. While initial cost estimates may cover startup expenses, depending on the complexity of a system, an extended support contract may be required for continued system utility from the vendor. Until an in-house solution is established to support these new systems, this may result in additional funding requirements. These potential problematic issues lead me to offer the hypothesis that successful implementation of a truly nationwide interoperable radio system will require DHS to grant supplemental funding to fiscally strained organizations. Another hypothesis drawn from these potential conflicts is that DHS may need to exercise mandatory regulation to ensure that all levels of emergency response reply to the interoperable communications initiative, which will streamline the desired results for improved disaster and response recovery

D. LITERATURE REVIEW

1. Introduction and Problem Statement

On July 6, 2012, President Barack Obama signed Executive Order (EO) 13618 for the "Assignment of National Security and Emergency Preparedness (NS/EP) Communications Functions."[1] This EO stressed the need for the federal government to provide a resilient communication infrastructure to effectively carry out emergency

[1] President Barack Obama, "Executive Order—Assignment of National Security and Emergency Preparedness Communications Functions, The White House (July 2012): http://www.whitehouse.gov/the-press-office/2012/07/06/executive-order-assignment-national-security-and-emergency-preparedness (accessed Sept. 12, 2012).

response and therefore ensure national security.[2] Although this EO was recently signed, it is the product of over a decade of planning in fulfilling one of the 9/11 Commission recommendations of developing a robust and interoperable Nationwide Public Safety Broadband Network (NPSBN).[3] The recent actions taken by the White House and DHS provide a unique opportunity for evolving technologies to contribute to the use of the NPSBN. When coordinated efforts have successfully been implemented at every level of public safety, interoperability practices and the sharing of intelligence can improve the way disaster response and recovery is carried out. Fortunately, this cooperative initiative is making progress; however, until it takes full effect, first responder organizations will continue to operate at a major disadvantage. In addressing this problem, analysis will be conducted on existing disaster response theory pertaining to inter-agency communications. Additionally, in order to summarize where interoperable communication efforts are currently headed and how they got there, government documentation will be primarily utilized due to its direct relevance and up-to-date accounting of program evolution.

2. Classic Disaster Response Principles–Views on Interoperable Communications

Although the concept of a nationwide effort to combine emergency response operations is fairly new at the federal level, the underlying principles of this initiative have been around for decades at the lower levels of emergency services. After a series of devastating wildfires hit southern California in 1970, Robert Irwin explained that the Incident Command System (ICS) was developed to improve emergency response and

[2] President Barack Obama, "Executive Order—Assignment of National Security and Emergency Preparedness Communications Functions, The White House (July 2012): http://www.whitehouse.gov/the-press-office/2012/07/06/executive-order-assignment-national-security-and-emergency-preparedness (accessed Sept. 12, 2012).

[3] "Written testimony of National Protection and Programs Directorate Office of Cybersecurity and Communications Deputy Assistant Secretary Roberta Stempfley for a House Committee on Homeland Security, Subcommittee on Emergency Preparedness, Response, and Communications hearing titled 'Resilient Communications: Current Challenges and Future Advancements,'" U.S. Department of Homeland Security (Sept. 2012): http://www.dhs.gov/news/2012/09/12/written-testimony-nppd-house-homeland-security-subcommittee-cybersecurity-0 (accessed Sept. 13, 2012).

coordination efforts when local agency resources were exhausted.[4] The planning process used in ICS is centered on allowing multiple agencies and emergency response personnel the ability to function as one organization to improve effectiveness, accountability and communications.[5] The commonality quality that ICS is based on first introduced the concept of establishing a single communications framework, creating a synergy of shared information, coordinated actions, and improved resource utilization.[6] An alternate view to establishing a single communications framework for emergency management is the belief that with a decentralized communication structure, multiple response options become available, representing a range of expertise.[7] According to risk communications expert Peter Sandman, allowing dissent in emergency planning encourages internal debate where hard decisions are worked toward, rather than promoting silence and complacency from a single coordinative authority in vital planning efforts.[8] By comparing these theories with relevant communication efforts, capability benefits and gaps can be analyzed in addressing the functionality of a nationwide interoperable radio network.

3. ISR Experience in the Battlefield

The seamless communication efforts that are being ordered by the White House and DHS are already being utilized in the battlefield. ISR data collected for mission planning is currently capable of being pushed to various coalition forces, allowing necessary access to key information.[9] Like DHS, the U.S. military puts a priority on personnel safety, battlefield SA, and interoperable communications. The much lighter

---

[4] Erik Auf der Heide and Robert Irwin, Disaster Response: Principles of Preparation and Coordination: C.V. Mosby Company (1989), 100.

[5] Ibid.

[6] Ibid., 116.

[7] Peter Sandman, "Dilemmas in Emergency Communication Policy," Emergency Risk Communication, Center for Disease Control and Prevention (2003), 19: www.psandman.com/articles/dilemmas.pdf (accessed Sept. 19, 2012).

[8] Ibid.

[9] Guy Norris, "Real-Time Intelligence, Surveillance & Reconnaissance (ISR) Data Sharing Technology for the "Af/Pak" Theatre," America At War (July 2009): http://afpakwar.com/blog/archives/1316 (accessed Apr. 09, 2012).

collaborative efforts the U.S. military needs to carry out these priorities are the main difference, given the fact that a battlefield is significantly smaller than the entire national public safety community. The utility of this common communications network has led to the increased use of shared ISR data to combat terrorist organizations. Intelligence is defined by the *Dictionary of United States Military Terms for Joint Usage* as "the product resulting from the collection, evaluation, analysis, integration, and interpretation of all available information which concerns one or more aspects of foreign nations or of areas of operation and which is immediately or potentially significant to planning."[10] Once the proper pipe, or network, is provided to the warfighter, it provides the means for accessing intelligence to complete critical mission objectives. Although this particular definition of intelligence is coined as a military term, the same message applies to public safety personnel. Like the warfighter, a first responder can also exploit information in such a way that it provides planning relevance through intelligence gathering for disaster response strategies. The successes of ISR implementation experienced in the battlefield are proving to be effective. White House counterterrorism adviser John O. Brennan addressed the nation in April 2012, stating that saving American lives and preventing terrorist attacks on the U.S. will require the U.S. to take part in targeted strikes using drones.[11] This vital counterterrorist tool is made possible through the use of ISR strategies and their exploitation over tactical data links, providing mission planning advantages and personnel safety. Although one would not initially think that an advantage in the U.S. war effort could raise negative attention, ACLU's Jameel Jaffar is an example of someone who is publicly speaking out against the drone program. According to Jaffar, President Obama has established a "bureaucratized killing program that will be available to every future president against every future enemy."[12] In addition

[10] Martin Bimfort, "A Definition of Intelligence," Central Intelligence Agency, Center for the Study of Intelligence (2007): https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol2no4/html/v02i4a08p_0001.htm (accessed Aug. 23, 2012).

[11] Greg Miller, "Brennan speech is first Obama acknowledgement of use of armed drones," The Washington Post (2012): http://www.washingtonpost.com/world/national- security/brennan-speech-is-first-obama-acknowledgement-of-use-of-armed-drones/2012/04/30/gIQAq7B4rT_story.html (accessed Aug. 30, 2012).

[12] Ari Shapiro, "Are Drones Obama's Legacy In War On Terrorism?" NPR (June 2012): http://www.npr.org/2012/06/20/155389081/are-drones-obamas-legacy-in-war-on-terrorism (accessed Sept. 19, 2012).

to this criticism, drone use has been blamed for excessive collateral damage in carrying out targeting attacks, placing a dark cloud over the ISR-driven striking platform that has gained the U.S. a comparable edge in the war against terrorism. At the moment, though, drones are a leading platform for ISR collection and have already influenced domestic law enforcement operations so much that the Federal Aviation Authority (FAA) estimates that 10,000 drones will be flying domestically by the year 2017.[13] Although unmanned systems are making progress in successful law enforcement and homeland security efforts, the negative attention being attracted in the battlefield may eventually limit their implementation domestically.

4. Emergency Preparedness and Response

Although internal communication standards are typically enough to conduct everyday independent operations, cross-agency communication interoperability is essential when a disaster strikes. Hurricane Katrina would come to be known as the most destructive natural disaster in U.S. history, claiming $96 billion in total damages and at least 1,330 casualties. [14] Adding to the destructiveness of Katrina was the paralyzing of communication infrastructures in the incident area. This served as a perfect use case for radio interoperability, whose shortcoming during this incident attracted national criticism. According to the Federal Response to Hurricane Katrina, "Ineffective communications between FEMA [Federal Emergency Management Agency] and other federal departments and agencies prevented available federal resources from being effectively used for response operations."[15] The lack of communication interoperability resulted in missed opportunities to utilize thousands of resources from federal and private agencies.[16] One of few communication successes that FEMA experienced was the use of their Mobile Emergency Response Support (MERS) detachments. However, although these

[13] Jeff Glor, "Drone use in the U.S. raises privacy concerns," *CBS News* (April 2012): http://www.cbsnews.com/8301–505263_162–57409759/drone-use-in-the-u.s-raises-privacy-concerns/ (accessed May 24, 2012).

[14] Executive Office of the President, "Federal Response to Hurricane Katrina," 8 (Feb. 2006): http://www.library.stmarytx.edu/acadlib/edocs/katrinawh.pdf (accessed May, 24 2012).

[15] Ibid., 45.

[16] Ibid.

systems successfully provided mobile communications, power generation, and potable water, only two of the possible five were used to support the catastrophe.[17] The lack of accountability in this instance leads to one of the many specific lessons learned expressed in "The Federal Response to Hurricane Katrina" report, recommending that DHS "Establish a National Operations Center to coordinate the National response and provide situational awareness and a common operating picture for the entire Federal government."[18] BLOS C2 capabilities speak directly to this recommendation, holding obvious value in future disaster response and recovery efforts. Another important consideration in disaster preparation is the potential for an intentional attack on U.S. critical infrastructure. On September 12, 2012, the Committee on Homeland Security's Subcommittee on "Cybersecurity, Infrastructure Protection, and Security Technologies" held a hearing on the possible threat of an electromagnetic pulse (EMP) and its potential consequences following the destructive "derecho" that hit Washington, DC, in 2012.[19] Spanish for the word "straight," a derecho is a term used to describe a widespread, long-lived, straight-line windstorm that is associated with a fast-moving band of severe thunderstorms.[20] This unfortunate incident took place on June 29, 2012, claimed the lives of 22 victims, and caused widespread damage that left millions of power outages from the Midwest to the Mid-Atlantic states.[21] This event once again exposed our weak emergency communications system and raised concern for future response. Both Hurricane Katrina and the Washington, DC, area derecho have subsequently demanded

[17] Executive Office of the President, "Federal Response to Hurricane Katrina,." 8 (Feb. 2006): http://www.library.stmarytx.edu/acadlib/edocs/katrinawh.pdf (accessed May, 24 2012), 44.

[18] Executive Office of the President, "Federal Response to Hurricane Katrina," 8 (Feb. 2006): http://www.library.stmarytx.edu/acadlib/edocs/katrinawh.pdf (accessed May, 24 2012), 36.

[19] Dan Lungren, "Subcommittee Hearing: The EMP Threat: Examining the Consequences," *U.S. House of Representatives Committee On Homeland Security* (Sept. 12, 2012): http://homeland.house.gov/hearing/subcommittee-hearing-emp-threat-examining-consequences (accessed Sept. 19. 2012).

[20] AccuWeather, "Intense Storms Called a "Derecho" Slam 700 Miles of the U.S." (2012): http://www.accuweather.com/en/weather-news/deadly-super-derecho-strikes-m/67383 (accessed Sept. 19, 2012).

[21] Jason Samenow, "Derecho: Behind Washington, D.C.'s destructive thunderstorm outbreak," June 29, 2012: http://www.washingtonpost.com/blogs/capital-weather-gang/post/derecho-behind-washington-dcs-destructive-thunderstorm-outbreak-june-29–2012/2012/06/30/gJQA22O7DW_blog.html (accessed Sept. 19, 2012).

attention regarding critical infrastructure protection and national security implications. Communications are a vital piece in responding to and recovering from a natural or intentional disaster, and U.S. history has provided more than enough material to draw on lessons learned and suggestions for future strategies.

5. Summary

The BLOS C2 capability is an NPS homegrown system used in JBAIIC experimentation for the past five years. Although there is limited literature specifically discussing this capability, information provided from the various components that make up BLOS C2, such as ISR integration and SA benefits, are used in this thesis. As for now, BLOS C2 is a system primarily intended to be used outside of the continental U.S. (OCONUS); therefore, examples have yet to be produced for use in the U.S. Through my assessment of DHS and local agency desired communication capabilities, I believe that the demand and interest in enhanced disaster response and recovery is more than enough to justify my major research question.

E. METHODS AND SOURCES

In approaching my major research question, I used various analytical approaches in reaching my conclusions. First and foremost, I used historical analysis to identify gaps in disaster response and recovery strategies. In this manner, I assessed the BLOS C2 capability's relevance for current homeland security demands. As mentioned in the literature review, major disasters in U.S. history, such as Hurricane Katrina and 9/11, provide a set of lessons learned that will have a visible effect on response strategy objectives. Additionally, historical analysis will reveal capability gaps that might have been overlooked in previous disaster response efforts, which can also offer debates used to come to a solution. Second, I used case studies to analyze existing disaster response strategies at all levels of government, and considered the benefits from integrating BLOS C2 capabilities. I initially looked into case studies at the federal level, analyzing the U.S. Coast Guard's communication systems in support of homeland security and disaster response. The military's use of interoperable radios and the ability to pass ISR data to ground, air, and sea coalition forces in theater provide an example of the BLOS C2

system's effectiveness in supporting the war effort. These examples are compared to the possibility of providing the same data utility at the domestic front. The next case study is at the state EMS level. The California Department of Forestry and Fire Protection (CAL FIRE) recently released its 2012 Strategic Plan highlighting the specific goals to promote firefighter safety, fireline situational awareness, and early surveillance.[22] After studying CAL FIRE's plans for achieving these goals and reviewing their existing communications framework, I considered the possible contributions that BLOS C2 can offer. The Salinas (California) Police Department (SPD) served as another case study, focusing on the local level of government interoperability efforts. Due to the department's recent transition of radio systems to the Harris Unity Next Generation (NGEN) P25 infrastructure that promotes interoperability, the BLOS C2 capability may also offer solutions in dealing with the city's growing gang violence issues. Lastly, these priorities have the potential to leverage BLOS C2 capabilities in fulfilling improvements to disaster response as well as internal operation efficiency. Through the use of these research methods, conclusions can be drawn from various aspects of available and potential data to address the major research question.

F. THESIS OVERVIEW

I first conducted an analysis of the DHS requirement to implement an interoperable emergency communication system to be utilized by public safety personnel. This required a focus on the federal, state, and local levels of emergency response in order to draw on the communications requirements necessary to accomplish the NPSBN through policy implementation. This led me into the case study of each level of emergency response. After looking at the U.S. Coast Guard (USCG), CAL FIRE, and the Salinas Police Department, I analyzed each organization's unique set of requirements in order to effectively assess opportunities for improvement and policy implementation needed for the integration of the BLOS C2 capability at each level. Once this was accomplished, I assessed each agency's potential to utilize of the BLOS C2 capability in

[22] California Department of Forestry and Fire Protection, "2012 Strategic Plan," 15 (2012): http://www.fire.ca.gov/about/downloads/Strategic_Plan/StrategicPlan_SinglePages.pdf (accessed Sept. 20, 2012).

carrying out improved disaster response and recovery. In wrapping up the case studies chapter, I drew upon a set of conclusions based on my findings. Drawing on these findings, my conclusion offers recommendations to DHS for improving disaster response and recovery at the coordinative federal level as well as the state and local levels. In closing of my thesis, I also provide future research recommendations as well as a concise conclusion summarizing the lessons learned in pursuit of my major research question.

II. ANALYSIS OF HOMELAND SECURITY EFFORTS AND REQUIREMENTS FOR INTEGRATION OF AN INTEROPERABLE EMERGENCY COMMUNICATIONS SYSTEM

In order for the BLOS C2 capability to aid in disaster response and recovery, an interoperable communications system is required at all levels of government to appropriately respond to disasters across the country. DHS has been working on the planning and implementation of a nationwide communications effort since 2001; in 2012, the Middle Class Tax Relief and Job Creation Act gave this program a boost by funding the Public Safety Communications and Electromagnetic Spectrum Auctions, funding the NPSBN.[23] This chapter focuses on what DHS has done to facilitate a nationwide interoperable emergency communications system, and analyzes whether it is enough to support the integration of BLOS C2 capabilities.

A. DHS OFFICE OF EMERGENCY COMMUNICATIONS

Both the 9/11 terrorists attacks and Hurricane Katrina highlighted communication shortfalls that resulted in emergency response failures. In response, Congress established a DHS Office of Emergency Communications (OEC) in 2007, partnering with all levels of government to improve emergency response communications. When President Obama updated the NS/EP communications responsibilities with Executive Order 13618, OEC and the former DHS National Communications System (NCS) consolidated efforts to improve emergency communications programs.[24] In an attempt to address all emergency communications issues, OEC focuses on supporting interoperable communications with existing technical capabilities for a comprehensive NS/EP architecture. Additionally, a DHS Emergency Communications Preparedness Center (ECPC) was established in 2009,

[23] "Nationwide Public Safety Broadband Network (NPSBN)," *Illinois First Net:* http://www.illinois.gov/firstnet/NPSBN/Pages/default.aspx (accessed Apr. 05, 2013).

[24] "About the Office of Emergency Communications," *U.S. Department of Homeland Security*: http://www.dhs.gov/about-office-emergency-communications (accessed Apr. 05, 2013).

representing the federal government's position in coordinating interoperable communications across emergency responder jurisdictions and functions.[25]

With the expansion of responsibilities given to OEC, a number of branches were added to the new division in order to support the coordination of interoperable emergency communications at all levels of government. The six branches include: 1) Policy and Planning; 2) Partnerships; 3) Regional Coordination; 4) Architecture and Advanced Technology; 5) Communications Portfolio Management; and 6) Technical Assistance Branches.[26] Each branch plays a part in successfully deploying a truly interoperable communications effort and making steady progress toward policy guidance and implementation.

Figure 2. Table displaying the formation of OEC by combining EO 13618 and NCS Title XVIII efforts. (From DHS/OEC website, June 2012)

1. Federal Oversight

Considering the magnitude of the OEC effort, DHS provided a substantial amount of support from a national point of view. In particular, the OEC Policy and Planning Branch provides policy recommendation and strategies for introducing new

[25] "Emergency Communications Preparedness Center," *U.S. Department of Homeland Security*: http://www.dhs.gov/emergency-communications-preparedness-center (accessed Apr. 05, 2013).

[26] Ibid.

communication technologies, while also providing assistance with emergency communications grant programs.[27] One strategy designed to guide the nation toward a standardized emergency communications platform is the National Emergency Communications Plan (NECP). This plan outlines specific response-level emergency communications goals for emergency responders to work toward, with performance metrics designed to evaluate agencies' interoperability capabilities in disaster situations.[28] The DHS website elaborates on this goal, stating that in order to successfully demonstrate response-level communications, "Each area must have common policies and procedures that allow interagency communications to occur consistently, clearly-defined responder roles and responsibilities that are maintained during an incident, and continuous, high-quality communications that are in place throughout the emergency or event."[29] With this concept in mind, the OEC Architecture and Advanced Technology Branch (AAT) serves as the principal emergency communications technical analysis representative, responsible for establishing an enterprise architecture as well as developing standards for emerging technologies that support emergency communications.[30] With standards being set in place for many DHS programs, the OEC Communications Portfolio Management Branch ensures that national security and emergency preparedness communications goals are the main focus. DHS programs such as the Government Emergency Telecommunications Service (GETS), Wireless Priority Services (WPS), Telecommunications Service Priority (TSP), and Next Generation Network Priority Service (NGN-PS) all serve to provide emergency responders with access to priority telecommunications services in order to have the appropriate infrastructure for responsive action.[31] The OEC Communications Portfolio Management Branch oversees these and other programs in order to ensure that

[27] "OEC Policy and Planning Branch," *U.S. Department of Homeland Security*: http://www.dhs.gov/oec-policy-and-planning-branch (accessed Apr. 06, 2013).

[28] "National Emergency Communications Plan (NECP) Goals," *U.S. Department of Homeland Security*: http://www.dhs.gov/national-emergency-communications-plan-necp-goals (accessed Apr. 06, 2013).

[29] Ibid.

[30] "OEC Architecture and Advanced Technology Branch," *U.S. Department of Homeland Security*: http://www.dhs.gov/oec-architecture-and-advanced-technology-branch (accessed Apr. 06, 2013).

[31] "OEC Communications Portfolio Management Branch," *U.S. Department of Homeland Security*: http://www.dhs.gov/oec-communications-portfolio-management-branch (accessed Apr. 06, 2013).

the directives and policies governing these projects are followed. With voice, data, and video at the forefront of the BLOC C2 utility, these prioritization programs are ideal in emergency situations where critical data will require substantial bandwidth to reach the appropriate personnel. These branches are important in establishing an overall interoperable communications framework, especially considering the variety of government and non-government stakeholders responsible for producing a reliable infrastructure and capability.

2. State and Local Oversight

With emergency communications stakeholders ranging from international to local partners, the OEC Partnerships Branch ensures that consistent emergency response improvements are taking place across all levels of government. Specifically, Statewide Interoperability Coordinators (SWIC) work to ensure that the Statewide Communications Interoperability Plans (SCIP) are being properly implemented in each state, while also acting as single points of contact for national interoperable emergency communication efforts.[32] DHS explains that, "SCIPs should outline and define the current and future vision for communications interoperability within the State or territory. In addition, SCIPs should align emergency response agencies with the goals, objectives, and initiatives for achieving that vision."[33] This formalized governance system helps create structures for future technology integration efforts, making up for the lack of standardization among two-way Land Mobile Radio (LMR) state emergency response users thus far. As of April 2008, all 56 states and territories had a department-approved SCIP, which not only encourages feedback, but also provides goals for successfully achieving statewide interoperability.[34] Understanding that each state faces unique challenges in fulfilling communication strategies, OEC also provides annual assessments of emergency preparedness communication capabilities and workshops that provide hands-on support to tackle state-specific SCIP initiatives. This governance and close

[32] "Statewide Interoperability Coordinators," *U.S. Department of Homeland Security*: http://www.dhs.gov/statewide-interoperability-coordinators (accessed Apr. 06, 2013).

[33] "Statewide Interoperability Plans," *U.S. Department of Homeland Security*: http://www.dhs.gov/statewide-communication-interoperability-plans (accessed Apr. 06, 2013).

[34] Ibid.

attention to states provides the oversight required to achieve a true NPSBN, avoiding the possibility of states falling behind by ignoring communication gaps.

Another way that OEC improves multi-jurisdictional and intergovernmental communications is through the SAFECOM Program. This program is a collaborative effort that draws on the expert opinions of more than 70 members, representing both the emergency responder and policy-making communities.[35] The SAFECOM program has contributed to the creation of guidance documents that have been instrumental in creating a clear path toward interoperable emergency communications for agencies at all levels of government. Additionally, state and local partners receive focused attention through the OEC Regional Coordination Program. This program assigns Regional Coordinators to each of the 10 Federal Emergency Management Agency regions, furthering the quality of feedback that OEC receives and emphasizing the emergency communications initiative.[36] One way that OEC is building close relationships with states and local entities is through their Interoperable Communications Technical Assistance Program (ITAP). Technical assistance offered by OEC not only reviews current methods and communication technologies, it also provides partners with the opportunity to engage in a number of service offerings through their Technical Assistance Catalog. These service offerings include workshops that focus on everything from planning to operational transitioning and technical development in order to cover all aspects of successfully implementing the OEC interoperable communications initiatives.[37] In addition to these on-site offerings, ITAP also provides partners with interactive online resources that cover a wide range of topics regarding the advancement of interoperable emergency communications nationwide. The online offerings include useful resources such as project management and radio technology training, references to OEC and Federal Communications Commission (FCC) documentation, and tools that aid in Frequency Mapping and Mobile

[35] "SAFECOM Program," *U.S. Department of Homeland Security*: http://www.dhs.gov/safecom-program (accessed Apr. 06, 2013).

[36] "OEC Regional Coordination Program," *U.S. Department of Homeland* Security: http://www.dhs.gov/oec-regional-coordination-program (accessed Apr. 06, 2013).

[37] "Office of Emergency Communications Technical Assistance Program," *U.S. Department of Homeland Security*: http://www.dhs.gov/office-emergency-communications-technical-assistance-program (accessed Apr. 06, 2013).

Data Surveys, just to name a few.[38] Transitioning toward the NPSBN means familiarizing state and local responders with the evolving technologies that promote interoperability. Through technical assistance and direct interaction with state and local actors, OEC is making progressive strides toward technical evolution and preparedness at a personal level.

Figure 3. The interactive OEC Technical Assistance homepage.

B. FIRSTNET

Another key contributor in the implementation of the NPSBN is the First Responders Network Authority (FirstNet), also funded by the Middle Class Tax Relief and Job Creation Act of 2012. Working with OEC, FirstNet in an independent authority out of the Department of Commerce's National Telecommunications and Information

[38] "Public Safety Technical Assistance Tools," *Interoperable Communications Technical Assistance Program*: http://www.publicsafetytools.info/start_index_v2.php (accessed Apr. 06, 2013).

Administration (NTIA), and is responsible for rolling out the NPSBN.[39] At a minimum, DHS explains, "FirstNet is responsible for ensuring nationwide standards for use and access of the network; and issuing open, transparent, and competitive requests for proposals (RFPs) to build, operate and maintain the network."[40] In order for interoperable emergency communications to be readily available during an emergency, a section of the radio spectrum is being secured for the NPSBN. This section is known as the "D Block," a 10 Megahertz (MHz) section of the radio spectrum, which will be dedicated to providing a network for emergency responders to pass crucial real-time data in the event of a disaster.[41] Placing the D Block adjacent to the existing 10 MHz section already dedicated to public safety (please refer to Figure 4), frees up a total of 20 MHz of radio spectrum solely intended for the use of emergency communications.[42]

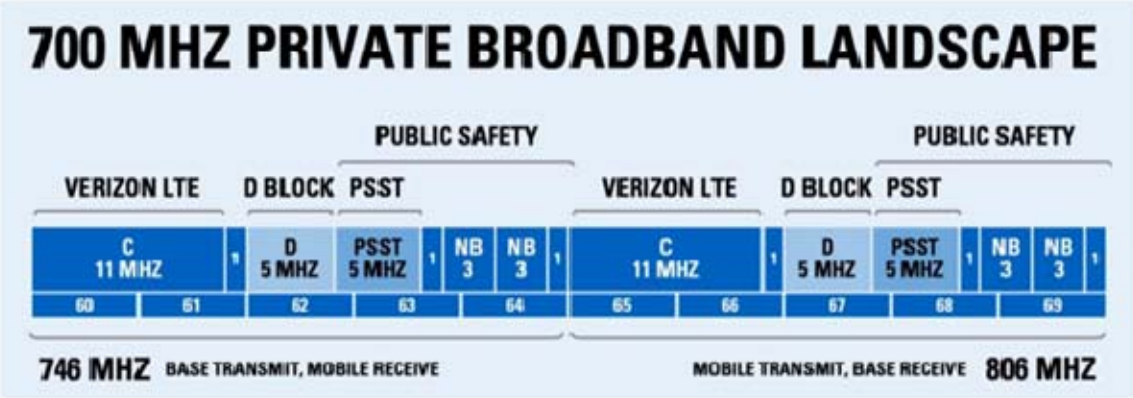

Figure 4. Diagram showing the 20 MHz dedicated to public safety and NPSBN in the 700 MHz frequency band. (Courtesy of Illinois FirstNet. n.d.)

[39] Chris Essid, "Nationwide Public Safety Broadband Network," *U.S. Department of Homeland Security* (June 2012): http://www.dhs.gov/sites/default/files/publications/Fact%20Sheet_Nationwide%20Public%20Safety%20Broadband%20Network.pdf (accessed Apr. 07, 2013).

[40] Ibid.

[41] Ibid.

[42] "Nationwide Public Safety Broadband Network (NPSBN)," *Illinois First Net:* http://www.illinois.gov/firstnet/NPSBN/Pages/default.aspx (accessed Apr. 05, 2013).

Not only does this landscape provide the capacity to communicate under the extreme network traffic environments brought about by emergencies, its location in the 700 MHz band also plays a major role in its reliability. The FCC elaborates on the benefits of the 700 MHz band, explaining, "The location of the 700 MHz Band—just above the remaining TV broadcast channels—give it excellent propagation characteristics. This allows the 700 MHz signals to penetrate buildings and walls easily and to cover larger geographic areas with less infrastructure (relative to frequencies in higher bands)."[43] These elements are extremely important given the uncertain conditions that emergency responders find themselves in once a disaster occurs. With this infrastructure in place, the urge for states and local entities to adopt interoperable communication systems is clear in order for them to participate in the data exchange. The availability and capacity of the NPSBN creates the perfect conditions for BLOS C2 capabilities to enhance the situational awareness picture that DHS and FirstNet have envisioned.

C. BLOS C2 INTEGRATION

Prior to researching existing nationwide interoperability efforts, establishing the necessary infrastructure to support domestic BLOS C2 capabilities appeared to present a number of organizational and financial obstacles. However, after learning about all the work over the past 10 years that has contributed to the planning of an interoperable emergency communications framework, plus the $7 billion going toward the building of the NPSBN, it appears as though BLOS C2 capabilities can leverage DHS' existing progressive efforts.[44] With this money going toward the building of the nationwide emergency response network and governance structure, BLOS C2 could utilize the network to produce a COP populated by sensor data pertaining to an emergency situation. Due to the interoperability efforts being implemented across multiple jurisdictions and

[43] "700 MHz," *Federal Communications Commission:* http://www.fcc.gov/topic/700-mhz (accessed Apr. 07, 2013).

[44] "The Nationwide Public Safety Broadband Network: First Steps," *U.S. Department of Homeland Security* (June 2012): http://www.dhs.gov/sites/default/files/publications/Case%20Study_Broadband%20FirstSteps.pdf (accessed Apr. 09, 2013).

agencies, useful data from these participants could flow across the network with little to no restrictions. The BLOS C2 capability would in turn make this data comprehensive and manageable by geo-referencing inputs and providing a level of situational awareness that could contribute to the success of emergency response. Although DHS is taking on the responsibility of deploying a nationwide emergency communication network, BLOS C2 would still require some ground-level integration in order to fully operate on the NPSBN architecture. This would have to be done once the initial architecture is in place in order for the systems to be tested and proven. The NPSBN makes it possible for the emergency responder community to benefit from BLOS C2 like the U.S. military has in its overseas endeavors. BLOS C2 has proven to be a desired capability for processing the large amount of ISR data produced overseas. Without a way to process data and manage assets, it is difficult to reap the full potential of their benefit to the mission. To assess the contributions that the BLOS C2 capability can offer emergency responders, we must look at federal, state, and local case studies to determine the support needed in order to deploy the capability, and whether it would be useful for disaster response at that level of government.

THIS PAGE INTENTIONALLY LEFT BLANK

III. CASE STUDIES FOR IMPLEMENTING BLOS C2 CAPABILITY

Once a disaster takes place, all levels of government are faced with the demand to interact in one way or another. In an effort to analyze the possible effects of BLOS C2 in improving disaster relief efforts, it is necessary to focus on individual organizations at the federal, state, and local levels in a series of case studies. The agencies that will be highlighted are the United States Coast Guard (USCG), CAL FIRE, and the Salinas Police Department (SPD). The USCG presents a unique opportunity to bridge gaps between domestic and armed forces response efforts given their status as the only military organization within DHS. CAL FIRE's interactions with federal wildland fire agencies also presents a number of possible opportunities to improve cooperative efforts pertaining to disaster response. Lastly, given the growing concern of gang violence in the Salinas Valley of Monterey County, the SPD may be able to benefit from SA capabilities in an effort to control limited as well as cooperative assets. These case studies analyze each agency's existing communications infrastructure in order to evaluate the requirements needed to implement the BLOS C2 capability. Once this is done, an assessment will be made on the potential impact of BLOS C2 on disaster response and recovery efforts as they pertain to homeland security. However, before I go into these specific case studies, I will explain the components that make up BLOS C2 and lay out its structure, functions, and services.

A. BLOS C2 EXPLAINED

1. Overview

Disaster situations create an array of data exchanges between various first responder agencies that contribute to time-sensitive relief efforts. Often, however, useful data does not make it to the right personnel at the right time, due to communication constraints that emerge from technological and physical boundaries. BLOS C2 addresses this capability gap through a network architecture that supports bi-directional information flows (FMV, still imagery, SA data, and voice and text chat communications) between air

and ground assets. This is carried out using various technological and administrative components that ensure interoperability among appropriate personnel and organizations. The result is an enhanced level of situational awareness (SA) that could aid in emergency response efforts.

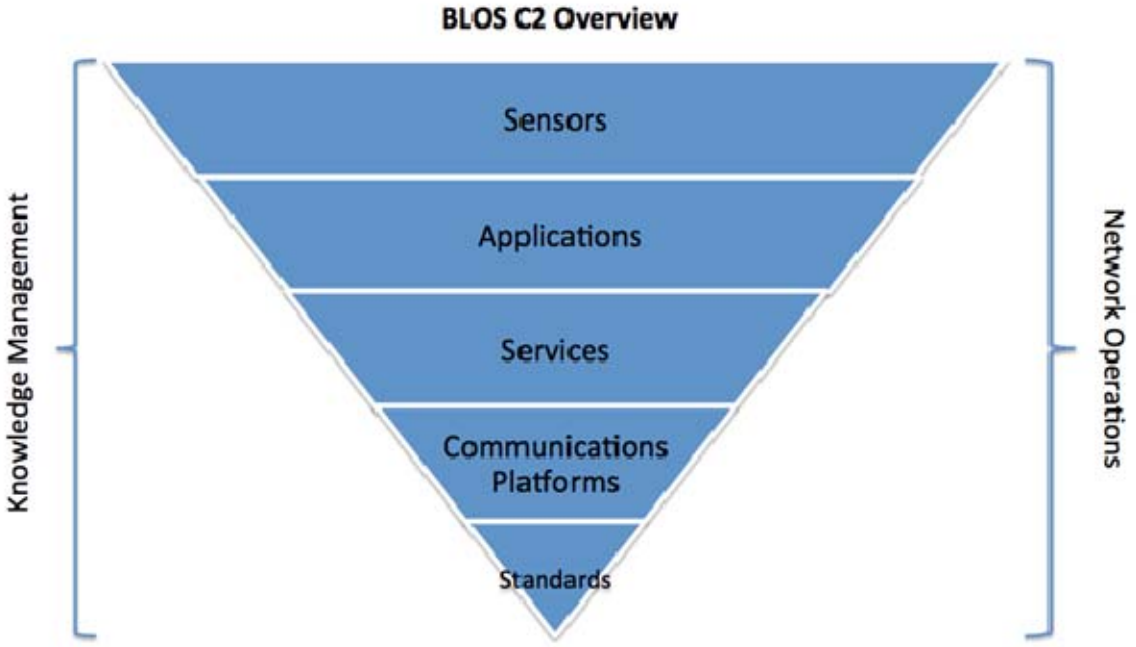

Figure 5. BLOS C2 Overview.

Figure 5 shows the five levels of the BLOS C2 architecture that support the operational effectiveness of the capability. Before a network topology can be erected to support the BLOS C2 picture, standards are required to govern the participants and parameters of the capability. This includes radio spectrum management, network protocols, policy, security, and messaging formats that outline the overall architecture of the system. These standards are the foundation of an interoperable capability aimed at supporting cross agency data exchanges and, once in place, could support specified communications platforms responsible for providing the data link for the information to pass through.

These platforms are made up largely of radios, but can also include telephones. These radios are the network's information highway, and promote interoperability

through the use of their software-defined digital radio protocols. The LMR technology that most agencies still rely on does not support Internet Protocol (IP) networking, limiting communications to strictly voice exchanges. In order to support all of the ISR information flows that contribute to the enhanced SA picture, high bandwidth, bi-directional, and IP capable network radios are required to push and pull the different types of data available. This capability is currently supported on the battlefield by U.S. forces through the use of Tactical Waveform IP radios. The implementation of P25 radios accomplishes the same objective domestically through a suite of standards for digital radio communications that enable federal, state, and local agencies to communicate with other agencies during emergency response efforts. The Ethernet interface on these IP radios allow users to connect their computer to the radio in order to use the data link to pass information such as video, SA tracks, and chat communications.

With respect to services that reside on the network, BLOS C2 incorporates terrestrially based servers for FMV and imagery processing, as well as a messaging infrastructure for event tagging and filtering. These servers interface with enterprise data sources (e.g., Automatic Identification System, Marine Transportation System) that provide a layer of information that can be used to enhance the SA picture. Additionally, the servers provide processing functionality with the ability to store large amounts of data, providing unique capabilities and services for network participants to utilize.

In order to access and pass information across these services and the network, BLOS C2 incorporates a software application suite that supports the C2 functionality and needs of the personnel responding to an emergency. These software applications include mapping, chat clients, voice clients, video players, Cursor on Target (CoT) tracking, as well as standard Windows applications. With the use of IP network-capable radios and the proper network configuration, users can connect their computers via a wireless or Ethernet interface to an IP radio and use the BLOS C2 software suite to exchange relevant data pertaining to an emergency over the BLOS C2 network. As an example, Figures 7 and 8 show the list of Windows applications that warfighters are currently using to pass critical information in the battlefield.

The last level that makes up the BLOS C2 infrastructure is the actual sensor data. These include enterprise data, FMV from aerial and ground Electro-Optical/Infrared (EO/IR) cameras, real-time positions of friendly and enemy locations, position of assets and critical infrastructure, and other relevant information that might be gathered. The sensor data is what makes the BLOS C2 capability really worthwhile, pushing the limits of traditional radio communications and providing useful data to the right personnel at the right time. The end result is an interoperable solution for communicating and displaying SA data along with real-time video and communications, enhancing the responder's awareness of the incident environment.

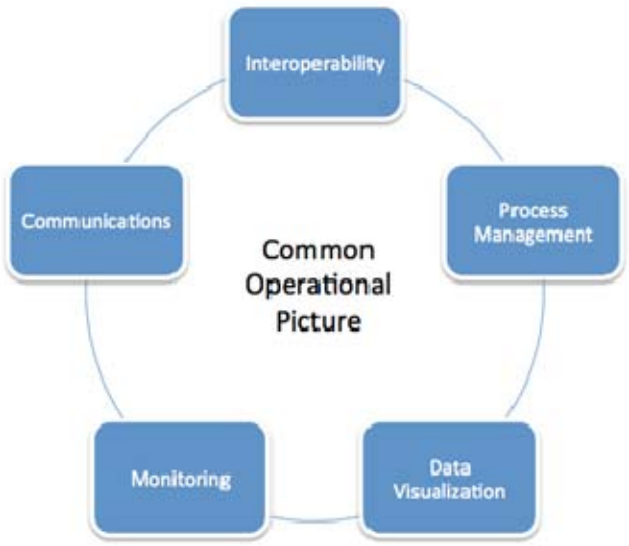

Figure 6. Components of a Common Operational Picture.

Application	Installed Version	Use/Function	Vendor	License Issue
Adobe Reader	11.0.0	Required for reading application documents and manuals	Adobe	Public Released
Collaborative Targeting	1.6	FalconView plugin that provides collaborative targeting functionality (collaboration on tracks across distributed teams)	MITRE	Government s/w
CoT Debugger	2.4.2 (2009.12.007 02:50)	Not geared for operational user, but needed as an engineering tool to support Cursor on Target (CoT) message format	MITRE	Public Released
CoT Moving Map Tool	2008.1.10 24f	Repositions map in FalconView based on own position	Macrovision	Part of BAO Kit
EtherView	4.8	Renders CoT messages on FalconView mapping application	SRA International	Part of BAO Kit
FireFox	16.0.2	Web browser (HTML 5) needed to support MARTI based image annotation	Mozilla Foundation	Public Released
FVCoT	1.4	CoT plugin for FalconView, required for Collaborative Targeting plugin	MITRE	Public Released
GeoChat	4.6	Provides low bandwidth (CoT-based) chat	SRA International	Part of BAO Kit
GetNineLine	4.7	Provides receiving/viewing of digital 9-Line message	SRA International	Part of BAO Kit
IPoL	0.7.20 (2011.09.08 02:32)	IP over legacy RF – used for low-bandwidth radio comms	MITRE	Part of BAO Kit
IPSetter	1.8	Sets IPOL's IP address based on configuration file	SRA International	Part of BAO Kit
Java	JRE 7 Update 9	Required for Transverse application	Oracle	Public Released
MARTI Plugin	4.1.1.1	Plugin for FalconView that allows user to generate geospatial queries into MARTI server and to receive FMV chips/imagery	AFRL	AFRL
NitfViewer	2.0.7.37	Imagery viewer for NITF format	NAWCPNS	Part of BAO Kit
PFPS (FalconView)	4.1.1	Mapping software for SA	GTRI (USAF)	Part of BAO Kit
RED	1.0	Application for displaying risk estimate distance and range rings in FalconView.	SRA International	Part of BAO Kit
Serial Port Splitter	3.6.3	Splits COM 3 port into 2 virtual comm ports	FabulaTech	Part of BAO Kit

Figure 7. BLOS C2 Software/Application List.

Services7	Jul 27 2011 14:13:59	Provides announcements and routing of message traffic	GMECI	Part of BAO Kit
ServicesToo	1.07 (16 Sept 09)	Older version of Services7, included as a backup	SRA International	Part of BAO Kit
SoldierSight Suite	1.4.2	FMV viewer and associated tools	L-3 Communications	BLOS C2
ST Toolkit	1.2.1	Allows generation of 9-Line, spot reports (i.e. drop icons on the map) and PPLI.	SRA International	Part of BAO Kit
STT MM	1.0	Moving map related application	SRA International	Part of BAO Kit
TGTS	1.2	App to communicate and validate a target or friendly location	SRA International	Part of BAO Kit
Transverse	1.7.3.2	XMPP-based chat client	AFRL	DoD s/w
VirusScan Enterprise	8.8 Patch 2	Antivirus	McAfee	DoD s/w
VLC Media Player	2.04	FMV viwer and tools – backup for SoldierSight	VideoLan	Public Released
WAVE Desktop Communicator	5.3	Desktop client for WAVE chat and VoIP	Twisted Pair Solutions	TacPod

Figure 8. BLOS C2 Software/ Application List (continued).

One of the main benefits that BLOS C2 contributes is the integration of a COP that can be shared across the network with appropriate personnel. As seen in Figure 6, the COP is made up of five functional areas that contribute to the SA gained from the overall picture. These functional areas are addressed by the five BLOS C2 architecture levels, providing the structure for an effective crisis-control solution. As previously noted, the ISR technologies that make up the BLOS C2 capability are currently fielded in theater and provide critical C2 that improves mission effectiveness. Through the use of ISR sensors that are populated into a COP, warfighters are currently able to visually track assets and subscribe to aerial FMV with the use of IP radios and strict process management practices. The interoperability gained through this system provides a common sharing platform that utilizes data being gathered from various agencies. After looking at case studies at the federal, state, and local government levels, this chapter examines the potential advantages of BLOS C2 capabilities could provide to improve emergency response and recovery at specific levels of government.

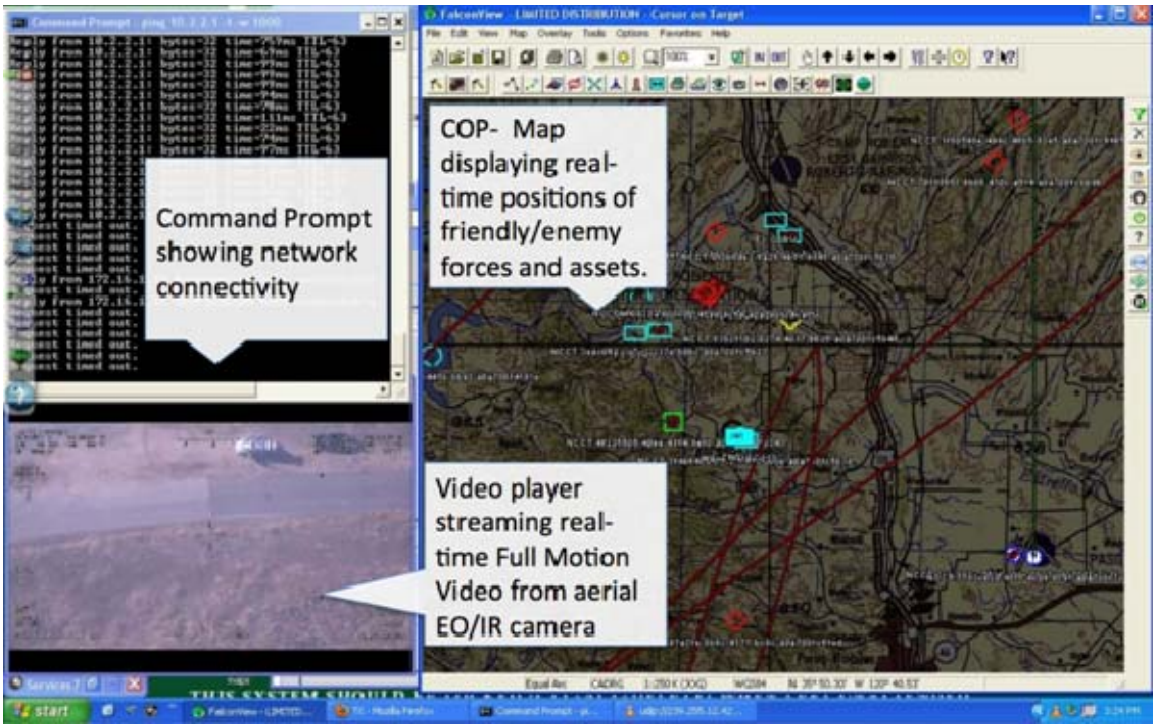

Figure 9. Screenshot of a user's computer screen with BLOS C2 capabilities.

B. U.S. COAST GUARD

> Attaining and sustaining an effective understanding and awareness of the maritime domain requires the collection, fusion, analysis, and dissemination of prioritized categories of data, information, and intelligence… Defeating terrorism requires integrated, comprehensive operations that maximize effectiveness without duplicating efforts.[45]
> USCG Office of Counterterrorism & Defense Operations Policy

1. Overview and Requirements

The United States Coast Guard (USCG) was placed under the DHS as a result of the Homeland Security Act of 2002.[46] Since the foundation of the agency, the USCG has focused most of its attention on defending the U.S. maritime environment as well as responding to those in peril. Given the broad geographic conditions facing the USCG,

[45] "Ports, Waterways, and Coastal Security (PWCS)," *United States Coast Guard* (2013): http://www.uscg.mil/hq/cg5/cg532/pwcs.asp (accessed Apr. 11, 2013).

[46] 107th Congress, "An Act to establish the Department of Homeland Security, and for other purposes," *Public Law 107–296-NOV. 25, 2002:* http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf (accessed Apr. 11, 2013).

continuous developments are always being made in strengthening its ability to detect and identify all activities in the maritime domain. This capability is known as Maritime Domain Awareness (MDA) and is a vital interest in safeguarding the homeland.[47] With this interest in mind, the USCG made strides toward updating boats and cutters (a vessel 65 feet in length or greater with live-aboard crew accommodations) to improve communications and implement emerging technologies. The Integrated Coast Guard Systems (ICGS) is focused on accomplishing these improvements by introducing three classes of new cutters and small boats, as well as manned and unmanned aircraft.[48] As an added benefit, the Unmanned Aerial Vehicles (UAVs) will be both land-based and cutter-based, increasing aircraft availability and data production. Additionally, the USCG assures that, "All of these highly capable assets are linked with Command, Control, Communications and Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) systems, and are supported by an integrated logistics regime."[49] These systems make for ideal BLOS C2 participants and make integration a matter of minor software configuration. Without the improvements being made by the ICGS initiative, USCG vessels would have limited mission effectiveness, especially in joint efforts. The USCG is also a big proponent of COP capabilities. The USCG has a program dedicated to developing a Common Operational Picture (COP), aiming to increase the amount of information available, as well as adding users and improving access methods.[50] With access to databases such as the Nationwide Automatic Identification System (NAIS) and the Long Range Identification and Tracking System (LRIT) used for vessel tracking, a COP can provide the USCG with a shared display of data capable of improving command

[47] "C3CEN Projects," *United States Coast Guard* (2013): http://www.uscg.mil/hq/c3cen/projects.asp (accessed Apr. 11, 2013).

[48] Ibid.

[49] Ibid.

[50] Ibid.

and control capabilities.[51] The U.S. military has a variety of data injections that could be used to populate the COP, which in addition to geographic locations can include information related to assets, activities, planning, environmental conditions, and ISR data. Additionally, with the EO/IR video sourcing from on-board UAVs, video can be shared with COP participants as long as the network is capable of handling the data packets. With the USCG taking the initiative in developing COP capabilities, BLOS C2 becomes another useful source of data in achieving mission objectives. To this end, once vessels receive the appropriate C4ISR interoperability upgrades, BLOS C2 should be able to contribute to the data being processed into the COP without requiring any major system changes.

2. Assessment

After taking a look at the USCG's existing communications infrastructure, it seems as though BLOS C2 capabilities can provide an added benefit in achieving the branch's core goals without making very many changes to the existing structure. One of the USCG's primary responsibilities is Ports, Waterways, and Coastal Security (PWCS), and due to the importance that this mission has for homeland security, I use the highlighted mission to assess BLOS C2's operational impact. According to the USCG website, "The PWCS mission entails the protection of the U.S. Maritime Domain and the U.S. Marine Transportation System (MTS) and those who live, work or recreate near them; the prevention and disruption of terrorist attacks, sabotage, espionage, or subversive acts; and response to and recovery from those that do occur."[52] In meeting these goals, the PWCS mission must carefully utilize USCG assets in order to completely achieve MDA on our waters. The MTS plays a vital role in maintaining the nation's economic health, supporting 99% of U.S. overseas trade and plays a critical role in

[51] Rayburn, "Written testimony of U.S. Coast Guard Deputy Commandant for Operations Vice Admiral Peter Neffenger for a House Committee on Transportation and Infrastructure, Subcommittee on Coast Guard and Maritime Transportation hearing titled 'A Review of Federal Maritime Domain Awareness Programs'" *U.S. Department of Homeland Security,* (July 2012): http://www.dhs.gov/news/2012/07/03/written-testimony-us-coast-guard-house-transportation-and-infrastructure (accessed May 11, 2013).

[52] "Ports, Waterways and Coastal Security (PWCS)," *United States Coast Guard.*

military mobilization.[53] Conducting PWCS creates preventative measures against terrorists who might target the MTS in an effort to damage a piece of our nation's critical infrastructure. In achieving MDA to protect the this critical infrastructure, BLOS C2 capabilities can not only aid in the consolidation of intelligence, but also expedite recovery efforts in the event of an attack.

The USCG relies on three primary methods of communicating between vessels and shore stations. These methods include Very High Frequency (VHF) Marine band radio, Medium Frequency/ High Frequency (MF/HF) Radiotelephone, and Mobile satellite radios.[54] VHF radios are the most relied upon communication method, intended for use between 5 to 10 miles of other vessels, and at least 20 miles to USCG shore stations.[55] VHF radios are also how the USCG receives distress calls from commercial and private vessels, and act as a party line allowing all channel participants to listen in on radio traffic.[56] In order to communicate at longer distances above 20 miles to several hundred miles, MF/HF radios are needed, requiring ideal antenna placement and substantial transmission power. This longer-range solution is useful for voice communications when VHF radios can no longer maintain a reliable link; however, its limited bandwidth does not substantially support other data formats such as video and still images. With the newer technology added to USCG cutters, the information being generated off shore could offer advantages to other users. Through the implementation of BLOS C2, the higher bandwidth VHF radio communications can sustain longer range while injecting the cutter sensor data into the overall USCG COP. This capability could potentially provide a layer of security and preparedness in the event of a MTS attack.

---

[53] Richard Lolich, "Marine Transportation System (MTS)," *U.S. Department of Transportation, Maritime Administration:* http://www.marad.dot.gov/ports_landing_page/marine_transportation_system/MTS.htm (accessed May 11, 2013).

[54] "Maritime Communications," *United States Coast Guard, Navigation Center* (2012): http://www.navcen.uscg.gov/?pageName=maritimeTelecomms (accessed May 15, 2013).

[55] "Radio Information for Boaters," *United States Coast Guard, Navigation Center* (2012): http://www.navcen.uscg.gov/?pageName=mtBoater (accessed May 15, 2013).

[56] Chuck Husick, "VHF Radios," *Boat U.S.* (Sept. 2009): http://www.boatus.com/husick/c_vhf.asp (accessed May 15, 2013).

The Mumbai, India, attacks carried out in 2008 by Pakistani terrorists accounted for approximately 160 deaths, and more than 308 injured.[57] In the aftermath of the attacks, it was reported that the terrorists inserted themselves into the country via small rubber boats, equipped with heavy backpacks that contained their weapons.[58] Although friendly countries border the U.S., this scenario is plausible and has been a DHS concern due to the difficulty to reliably detect this method of insertion along our vast coastlines. This tragic event highlights the need for enhanced MDA, especially considering the implications that this attack has on human life and the security of our ports and waterways. The BLOS C2 capability could aid in achieving MDA through prevention and response.

Although the USCG practices the screening of vessels and crews, random boardings, and increased patrols of critical infrastructure, an operational need for enhanced SA exists. Under the ICGS initiative discussed earlier in this case study, it is reported that the UAVs will be added to the USCG's assets. These UAVs will obviously be able to aid in the increased patrolling of critical infrastructure, but they will also offer the capability of detecting suspicious activity with ample time to allow a boarding before a docking can take place. Supported with C4ISR interoperable systems, these UAVs will be equipped with the necessary tools to produce valuable data for MDA. BLOS C2 could help in the application of this data by providing the utility of video distribution and storage. With FMV originating from a cutter or shore-based UAV, agencies outside of the USCG will want to access the captured information. Through a computer networking process known as multicast, BLOS C2 can deliver the UAV FMV to a group of approved destination computers simultaneously in a single transmission. This capability improves fusion efforts that promote information sharing, which is a top DHS priority since the

[57] Mark Magnier and Subhash Sharma, "Terror attacks ravage Mumbai," *Los Angeles Times* (Nov. 27, 2008): http://articles.latimes.com/2008/nov/27/world/fg-mumbai27 (accessed May 15, 2013).

[58] "TDC Security Alert: Maritime Aspects of Mumbai Terror Attacks," *The Maritime Executive* (Dec. 04, 2008): http://www.maritime-executive.com/article/tdc-security-alert-maritime-aspects-mumbai-terror-attacks/ (accessed Apr. 15, 2013).

release of the 9/11 commission report.[59] This means that, in the process of conducting routine UAV patrols of a given area, the appropriate agencies have the opportunity to compare and provide additional information that may have not been considered by the originating agency. Tips and communication interceptions are not always broadcasted for all agencies to weigh in on, creating gaps in intelligence gathering that can allow attacks to be carried out under the radar. Through the multicasting of USCG drone video, these types of gaps are constricted, allowing for more opportunities to prevent malicious activities such as an attack on the MTS. Additionally, BLOS C2 offers the capability of storing FMV in large capacities. This not only helps with performing after action analysis of captured events, but it also aids in the ability to compare and detect behaviors that take place over long periods of time. In addition to these preventative measures, the BLOS C2 capability can also aid in response efforts using this same scenario.

In the event that a disaster would occur on a MTS component, USCG response efforts could be improved with the implementation of BLOS C2 in the existing ICGS upgrade plan. Although the USCG already has a COP program used to create SA, BLOS C2 could collaborate data inputs outside of USCG in order to enhance the SA picture. With contributions from joint agencies in response to a disaster, response strategies can be managed properly by avoiding the duplication of efforts from multiple organizations. This is especially important when resources are limited and attention is required on multiple fronts. With the MTS being considered as critical infrastructure, it is imperative that disaster response be performed in the most efficient manner possible. BLOS C2 not only proposes efficiency in managing the data populating the COP, it also promotes the efficient management of collaborative assets and efforts in the event of a disaster. Figure 10 represents the current USCG communications capability, while Figure 11 displays a broad overview of how BLOS C2 could improve USCG communication and data sharing in the scenarios presented in this case study.

[59] National Commission on Terrorist Attacks upon the United States (2004). *The 9/11Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*. Washington, DC.

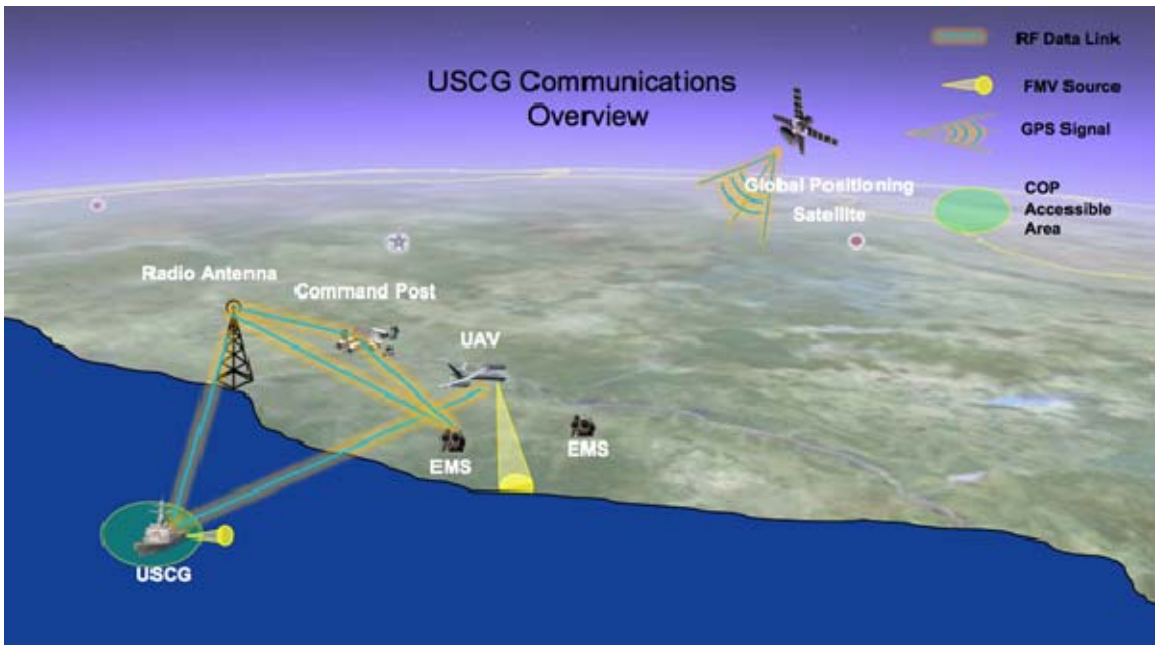

Figure 10. USCG/ ICGS communications overview and without BLOS C2 implemented.

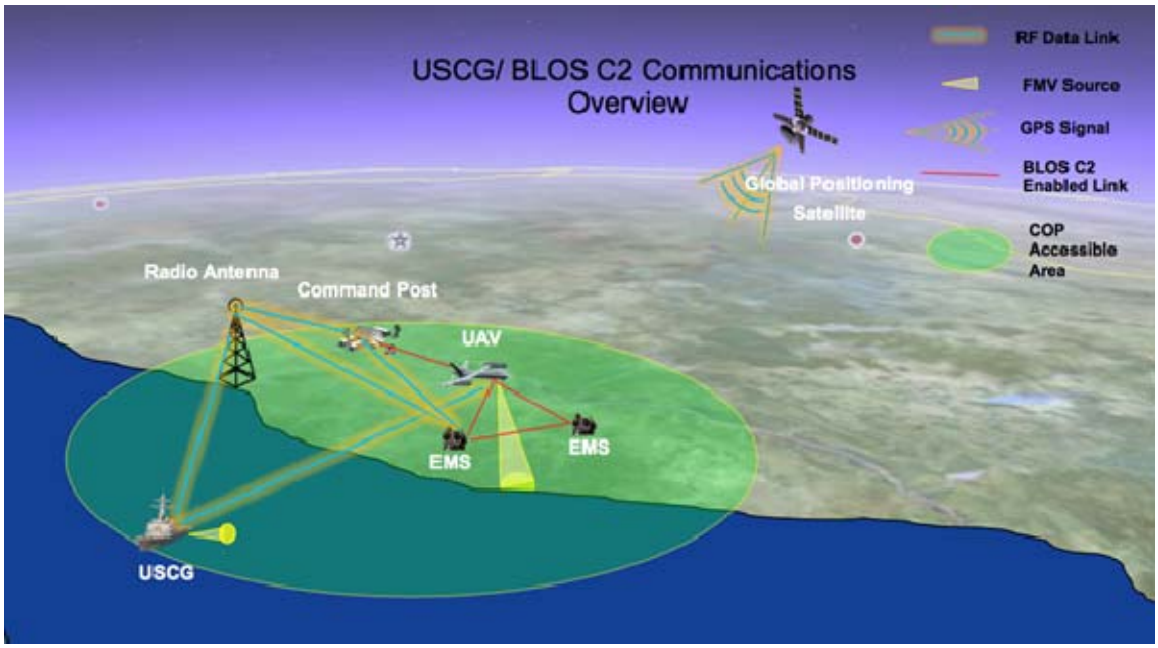

Figure 11. USCG communications overview using BLOS C2.

Although the two figures have the same nodes present, the information routes and distribution of data is different. As can be seen in Figure 10, the UAV is gathering FMV data; however, it is only able to share the information with the cutter from which it launched. This excludes the command post and emergency responders on the ground from accessing the data, because the processing capability (BLOS C2) is not present. Additionally, SA data is limited to the USCG COP in the existing communications framework as seen in Figure 10. However, once BLOS C2 technologies are implemented, as shown in Figure 11, the COP is extended to all ground users within USCG as well as cooperative agencies. Even though all of the nodes can maintain voice communications in the current architecture, FMV viewing can offer substantial benefits for all supporting agencies. Once the BLOS C2 capability is introduced into the architecture, multiple users can then view the FMV from the cutter UAV through the BLOS C2 enabled link supported by the NPSBN and NGEN radios. Accurate positioning of each node is provided by real-time GPS tracking, which can be seen in both figures, validating the information that is being displayed in the COP. The USCG is on an aggressive path toward interoperability and MDA with the use of COPs and upgraded assets; however, through the use of BLOS C2, their current efforts could achieve greater mission effectiveness as seen in this case study.

C. CAL FIRE

> In a state as large and populated as California, cooperative efforts via contracts and agreements between state, federal, and local agencies are essential to respond to emergencies like wildland and structure fires, floods, earthquakes… and even terrorist attacks. Because of these types of cooperative efforts fire engines and crews from many different agencies may respond at the scene of an emergency. California Department of Forestry and Fire Protection, "What is CAL FIRE?"[60]

1. Overview and Requirements

The California Department of Forestry and Fire Protection's (CAL FIRE) mission statement is, "to serve and safeguard people by protecting California's property and

[60] "What is CAL FIRE?" *California Department of Forestry and Fire Protection:* http://www.fire.ca.gov/communications/downloads/fact_sheets/WhatisCALFIRE.pdf (accessed July 02, 2013).

resources from fire." Serving 35 of California's 58 counties, CAL FIRE faces ongoing challenges due to unpredictable environmental conditions and a growing population.[61] On average, CAL FIRE reportedly "responds to more than 5,600 wildland fires that burn over 172,000 acres each year. In addition, department personnel answer the call more than 350,000 times for other emergencies including structure fires; automobile accidents; medical aids; swift water rescues; civil disturbances; search and rescues; hazardous material spills; train wrecks; floods; and earthquakes."[62] The workload taken on by CAL FIRE has contributed to its positive reputation and dependability, giving the department the opportunity to assist in response efforts with federal and local agencies. Not only is this collaboration useful in creating cross-agency partnerships, it is also absolutely necessary in order to appropriately respond to national disasters. With the level of cooperativeness that CAL FIRE has adopted, it is without a doubt that their services would be summonsed and necessary in the event of a terrorist attack in or around the state of California. Currently, CAL FIRE's rapid response solution for establishing communication capabilities on the move is through their Mobile Communications Centers (MCC). The MCC provides a mobile hub for communications activity and allows dispatchers to monitor the incident radio traffic on site and coordinate with local Emergency Command Centers (ECC).[63] The communications equipment provided on the MCC include: 10 channel dispatch consoles with VHF, UHF, Low Band, 800 MHz, and VHF-AM radios, Satellite telephones, an amateur (HAM) radio station, and a 30-foot pneumatic antenna mast that can be seen in Figure 12.[64] This equipment is provided in a mobile platform in order to respond to disasters in remote areas, relying on satellite connectivity to pass voice communications when the other tower-dependent radios are out of reach. In addition to the 5 MCCs currently in service, CAL FIRE also operates

[61] What is CAL FIRE?" *California Department of Forestry and Fire Protection:* http://www.fire.ca.gov/communications/downloads/fact_sheets/WhatisCALFIRE.pdf (accessed July 02, 2013).

[62] Ibid.

[63] "CAL FIRE Mobile Communications Center (MCC)," *California Department of Forestry and Fire Protection* (April 2011): http://www.fire.ca.gov/communications/downloads/fact_sheets/MCC.pdf (accessed July 02, 2013).

[64] Ibid.

over 1,000 fire engines, 63 paramedic units, 215 rescue squads, 11 helicopters, and 13 air tactical planes among other support equipment. [65] With the entire state of California to serve, CAL FIRE demands the efficient distribution of this equipment in order to effectively carry out its protective initiatives.

Figure 12. CAL FIRE MCC (Images retrieved from CAL FIRE website). April 2011.

In 2012, CAL FIRE released its Strategic Plan highlighting the specific goals required to improve the department's performance amidst changes in fire protection demands and technological advancements.[66] The initiatives listed throughout this strategic plan are in response to mandates that call for improved management of monetary and personnel resources while maintaining the overall success and efficiency of the organization. One suggestion provided in the Strategic Plan that specifically speaks to the integration of the BLOS C2 capability is the objective to utilize evolving technologies to benefit the following fire protection priorities: "firefighter health and safety, fireline situational awareness and status (including Automated Vehicle Location (AVL)

[65] "What is CALFIRE?" California Department of Forestry and Fire Protection.

[66] "2012 Strategic Plan," California Department of Forestry and Fire Protection (2012), 15.

technology and supporting software/hardware), and early surveillance (e.g., aerial cameras and drones with thermal imaging and store and record capabilities)."[67] Intended to take the department through the year 2017, CAL FIRE's Strategic Plan in conjunction with the NPSBN could offer an ideal environment for BLOS C2 integration. Once integrated into a support unit such as a MCC, BLOS C2 could aid the dispatch role by improving radio reliability along with the benefits of a Common Operating Picture (COP). With these benefits taking effect, CAL FIRE could increase interoperability with cooperative agencies and operate more efficiently in remote areas, improving response tactics used to support disasters that could threaten homeland security.

2. Assessment

As mentioned in the overview, CAL FIRE's response to more than 5,600 wildland fires every year demand the need of a plan to efficiently manage their distributed equipment and a staff of 4,700 full-time fire professionals.[68] To accomplish this, the 2012 Strategic Plan paves the way for the identification of technologies related to fulfilling fire protection priorities. Serving over 31 million acres, the need to coordinate assets and operations is vital in carrying out the CAL FIRE mission and ensuring firefighter safety.[69] CAL FIRE could improve coordination efforts with a BLOS C2 capability through the use of a COP populated by various relevant data sources such as real-time video and GPS tracking provided by the AVL technology. With the distribution of a COP across the department and cooperative agencies, tracking and requesting additional resources and personnel becomes easier to manage. The C2 gained from this SA picture could vastly improve not only firefighter safety, but fireline SA as well. The nature of wildfires and their geographic hurdles can make this task especially difficult for tower dependent/line of sight communications. Through the utilization of interoperable radios such as P25 NGEN radios with trunking and GPS capabilities, user location is provided to all subscribers on a specified channel over the secure network. Additionally,

[67] "2012 Strategic Plan," California Department of Forestry and Fire Protection (2012), 15.

[68] "CAL FIRE at a Glance," California Department of Forestry and Fire Protection (Dec. 2009): http://www.fire.ca.gov/communications/downloads/fact_sheets/Glance.pdf (accessed July 02, 2013).

[69] "What is CAL FIRE?" California Department of Forestry and Fire Protection.

LOS communications can be extended through the use of radio access points onboard CAL FIRE aerial assets. This would provide critical range extension for communications in areas with geological boundaries that prevent users from establishing a reliable link. Physical boundaries can become less of an inhibitor in carrying out C2 communications once this capability becomes available, allowing for the accountability of personnel in nearly any environment. Finally, with access to aerial sources of video such as thermal imaging, early detection and fireline status can be delivered to firefighters and first responders in less time, minimizing total loss of fire destruction.

To understand how BLOS C2 capabilities can directly improve CAL FIRE's emergency response plan, I will be applying the benefits to a scenario that would call on CAL FIRE to work cooperatively with other agencies to showcase the potential of the capability. With a terrorist's primary objective revolving around the notion of creating widespread fear, it would not be unrealistic to assume that state and national forests would be potential targets. Whether a wildfire was a terrorist's primary objective or a result of a bombing, CAL FIRE would be required to respond in the same manner. As with any forest fire, detection is a vital component in assessing and responding to the incident. Equipped with existing EO/IR cameras, CAL FIRE aerial assets could properly diagnose fire severity as well as response requirements from that vantage point. This is an existing capability; however, BLOS C2 could provide secure multicast capabilities to ground users just as it would in the USCG model, keeping approved personnel in the loop and denying access to all others. Figure 8 demonstrates how the video is tunneled directly back to the dispatch center in the current framework, while Figure 14 displays the ability to publish the useful video to ground subscribers with the implementation of BLOS C2 capabilities. Video SA would allow CAL FIRE and cooperative departments, ranging from federal and local branches, to further engage in the overall response effort. Additionally, if terrain is a limiting factor in passing reliable voice communications and other sources of data such as FMV, BLOS C2 assets could extend the range of communication through the use of repeaters on CAL FIRE aerial assets (refer to Figure 14). This solution is reconfigurable due to the mobility of the aircraft and also much more reliable than satellite communications that only support low bandwidth data exchange.

Lastly, with the threat of terrorist involvement, a COP can assist in providing a map of where EMS personnel and equipment are located, as well as references of where potential terrorists or "red forces" are thought to be located. Without the presence of BLOS C2 systems, a COP is not supported in CAL FIRE's communication architecture. However, as seen in Figure 14, once implemented, COP SA data could cover the entire incident area. GPS-enabled radios and CAL FIRE AVL technology provide the availability of these data injections, in addition to user inputs that share information regarding other useful elements such as environmental hazards. Currently, geographical boundaries place limitations on emergency responder line of sight (LOS) land mobile radio communications due to their tower dependency. Although Low Earth Orbit (LEO) and satellite phones provide worldwide coverage for the most part, this method of communication is limited to primarily voice communications, ruling out their use in architectures that require larger data exchanges. Figure 13 depicts this dilemma by showing how supporting agencies may be denied communications with other departments responding to the same incident due to LOS-deprived environments. The NPSBN would ensure that supporting departments could seamlessly participate in mission communications and also provide COP capabilities far beyond CAL FIRE's sole visibility. This would provide cooperative agencies with the necessary tools to join and assist in disaster response efforts under the condition that they comply with the interoperability standards set in place by DHS. With terrorist organizations exploring potential U.S. targets, it is fair to say that BLOS C2 could potentially limit the damage brought about by malicious attacks on state and local forests.

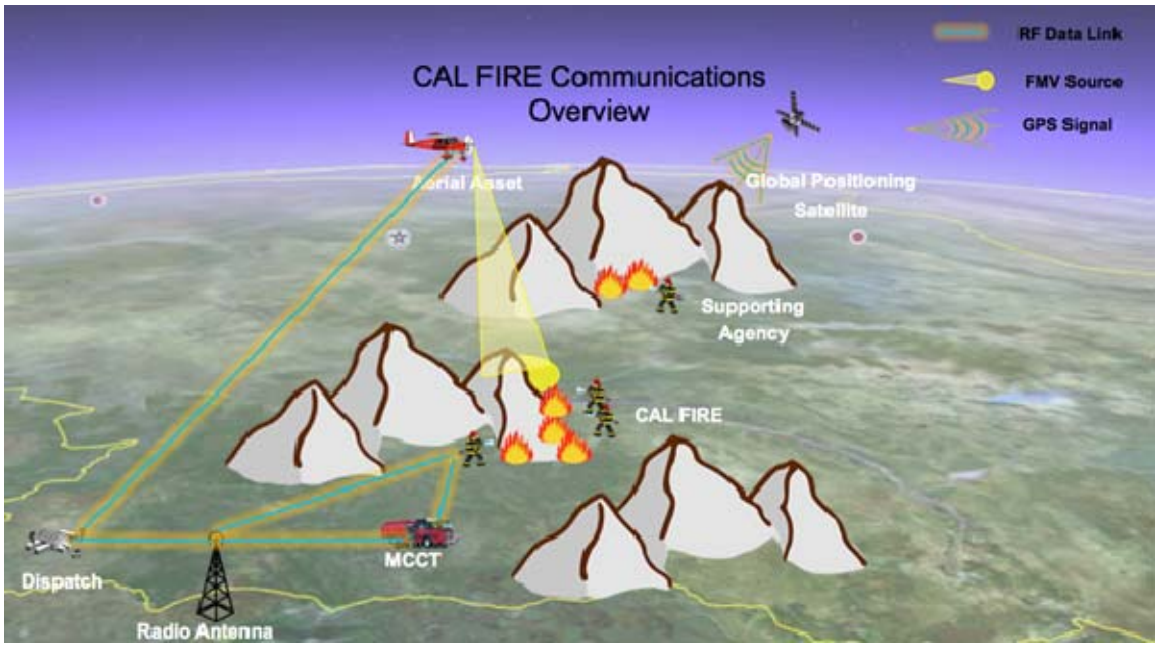

Figure 13. CAL FIRE Communications Overview with Existing Architecture.

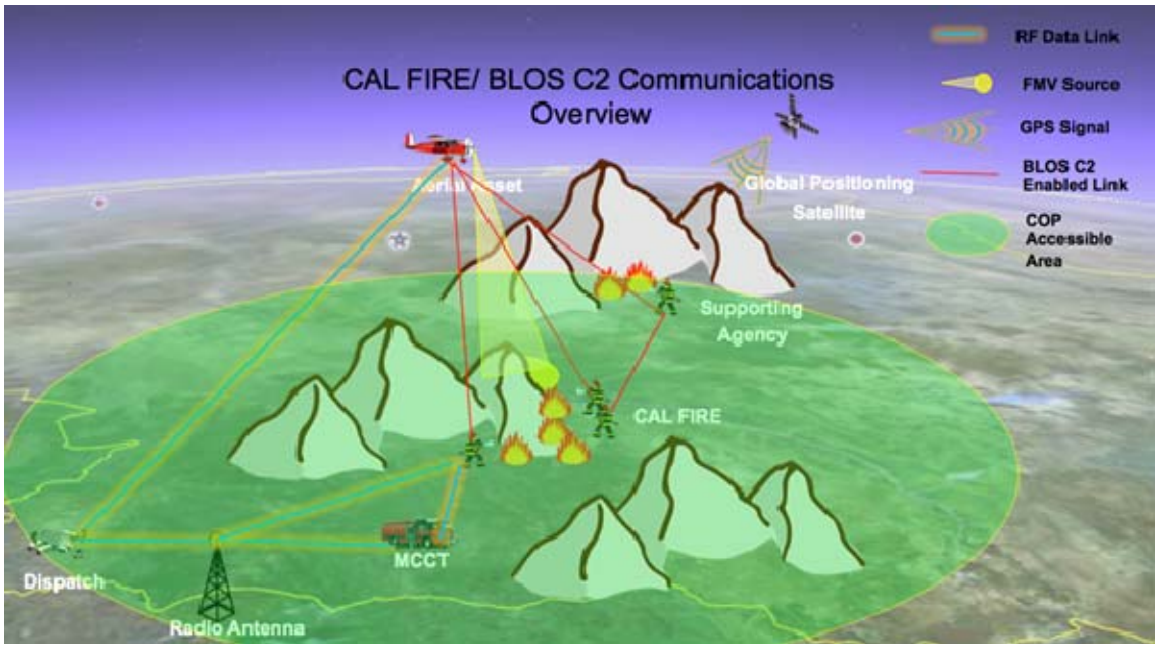

Figure 14. CAL FIRE Communications Overview with BLOS C2 Integrated Capabilities.

While the NGEN communications capabilities cover statewide firefighting efforts, they will also potentially satisfy national DHS initiatives. In adopting NGEN P25 radios, CAL FIRE can benefit from BLOS C2 capabilities while moving in the direction of complying with the DHS-mandated nationwide public safety broadband network initiative (NPSBN). When communications are denied due to a disaster, inter-agency cooperation and network deployment become the highest priorities in coordinating large-scale emergency responses. This is especially true if terrorist actions are involved, making recovery efforts time sensitive. With the implementation of the NPSBN, BLOS C2 can potentially bridge relevant first responders under one network, while publishing critical data that can lead to more efficient response and recovery. This capability speaks directly to the requirements described in the 2012 CAL FIRE Strategic Plan as well as the Department of Homeland Security NPSBN initiative, and can offer advantages that have been tested and experienced by U.S. military in the battlefield.

D. SALINAS POLICE DEPARTMENT

> Working in partnership with the people of Salinas to enhance the quality of life through the delivery of professional, superior and compassionate police services to the community.
>
> —Salinas Police Department Mission Statement

1. Overview and Requirements

Responsible for over half of the lettuce grown in the U.S., the city known as the "Salad Bowl" has received national attention for more than just lettuce production over the years.[70] In 2009, the city of Salinas reportedly had a homicide rate that was four times that of the national average, accounting for 29 murders by the end of the year.[71] The growing gang influence in Salinas is completely responsible for these figures, placing

[70] Paul F. Griffin and Langdon White, "Lettuce Industry of the Salinas Valley," *The Scientific Monthly*,81.2, 77. (1955): http://ccwg.mlml.calstate.edu/sites/default/files/projects/gabilanHEP/griffinwhite_1955_lettuce_industry_salinasvalley.pdf (accessed May 05, 2013).

[71] Louis Fetherolf, "Message from Chief Louis Fetherolf." *Salinas Police Department Report to the Community*, July 1, 2010: http://news.salinaspd.com/index.cfm/Message_from_Salinas_Police_Chief_Louis_Fetherolf_4358.htm#.UjNygRZ41QU (accessed July 11, 2013).

local law enforcement at the center of the problem. Taken from its website, "The Salinas Police Department (SPD) has a staff of 149 sworn and 58 non-sworn personnel, an authorized sworn strength of 187 police officers, and an annual budget of $18 million." [72] SPD's manning took a hit in 2010 when the city of Salinas faced a budget crisis, forcing the chief of police to cut 19 sworn officer position as well as seven staff members.[73] This reduction of police workforce only added to the city's crime issues, deploying fewer patrol officers while the gang community continued to grow. To provide an idea of what the department is up against, SPD responds to an average of 8,500 calls for service each month, to a community of over 160,000 residents.[74] These numbers contribute to the raised awareness of SPD's understaffing issues, becoming a cause for concern in the "Salinas Comprehensive Strategy for Community-wide Violence Reduction," released in 2010. This strategic plan pointed out that in 2008, the city of Salinas was listed as having 1.23 full-time police officers per 1,000 residents compared to the California average of 2.56 officers per 1,000.[75] Additionally, crime data collected by the Federal Bureau of Intelligence (FBI) indicates that Salinas' violent crime rates are among the nation's highest, occurring at the frequency of 7.3 per 1,000 residents compared to the national average of 3.9 per 1,000.[76] The result of these statistics leads to the realization that the city's considerably high crime rates are simply too demanding for the short-handed SPD.

In conducting day-to-day police operations, officers are supported with standard technical policing devices that aid in communications and surveillance to a certain degree. During a typical shift, an officer utilizes the following technological equipment: a vehicle-mounted mobile data terminal (MDT), a vehicle mounted/ portable land mobile

[72] "Employment with the Salinas Police Department," *Salinas Police Department* (2013): http://www.salinaspd.com/employment-general (accessed July 11, 2013).

[73] Fetherolf. "Message from Chief Louis Fetherolf."

[74] "Employment with the Salinas Police Department," *Salinas Police Department* (2013).

[75] Georgina Mendoza, "Salinas Comprehensive Strategy for Community-wide Violence Reduction," *City of Salinas:* http://www.ci.salinas.ca.us/pdf/SalinasSWP.pdf (accessed July 15, 2013).

[76] "Crime rates for Salinas, CA," *Neighborhood Scout* (2013): http://www.neighborhoodscout.com/ca/salinas/crime/#data (accessed July 15, 2013).

radio (LMR), and cellular phones.[77] Other assets that officers have limited access to are five Closed Circuit TVs (CCTV) and a Mobile Command Vehicle (MCV). The five CCTVs are closed circuit mobile cameras that conduct surveillance on known problematic areas. Although the CCTVs have the potential to improve response efforts, their main purpose is to extend police presence without physically locating an actual police officer at the site. The MCV was initially intended to support high-risk events that required advanced command and control (C2); however, the lack of computing and communications equipment has stripped the response vehicle of its operational value.

In order to comply with the larger DHS efforts to implement the NPSBN and offer the ability to integrate BLOS C2 technologies, SPD would need to vastly improve its communications infrastructure as well as more fully utilize existing assets that could offer benefits in carrying out police efforts. Some of these requirements have already been initiated with the help of grants from state and federal entities including the U.S. Department of Justice and DHS.[78] The capabilities that are being pursued due to availability of grant funding include the procurement of 200 portable and 70 handheld vehicle-mounted broadband NGEN radios and the outfitting of patrol vehicles with 3G wireless Internet connectivity for MDT implementation.[79] Although these improvements affect SPD's ability to move forward with NPSBN initiatives, the integration of these new technologies need to stretch beyond satisfying DHS communications standards in order to help respond to the demands of the severe gang problem facing the city.

2. Assessment

In addition to efforts revolving around community involvement and local response strategies, SPD has openly requested assistance from allied agencies in response to dramatic spikes in violence. In 2013, SPD issued a request for help in carrying out a

[77] Jerome Dubay, "Implementing Joint Battlespace Awareness IST Integration Capability Architecture: A Crime-Reduction Strategy in Salinas, California," (master's thesis, Naval Postgraduate School, June 2011): Print, 37.

[78] Julia Reynolds, "NPS System Gives Salinas Police Field Data in Real Time," *The Monterey Herald* (August 30, 2012): http://www.montereyherald.com/local/ci_21440031/nps-creates-system-that-gives-salinas-police-field (accessed July 16, 2013).

[79] Dubay, "Implementing Joint Battlespace Awareness," 75.

"City Wide Directed Enforcement" that would target gangs and their members who were known to have been involved in criminal activity.[80] In response, on August 2, 2013, 70 officers participated in the operation, representing state and federal law enforcement agencies such as Alcohol Tobacco and Firearms, Federal Bureau of Investigations, Homeland Security Investigations, United States Marshall's Office, and California Highway Patrol.[81] The cooperation of these agencies was crucial in successfully carrying out the operation that would ultimately result in the arrests of 10 known gang members while conducting 10 residential searches, over 70 traffic stops, and numerous pedestrian checks.[82] The success of this effort highlights the need to continue with the implementation of NPSBN interoperable communication standards at the local level. Additionally, this operative further highlights DHS' recognition that the presence of gang activity in Salinas presents a significant threat to public safety that requires attention. With ongoing assistance taking place in Salinas from allied law enforcement agencies, the use of BLOS C2 capabilities could enhance the cooperative efforts aimed at reducing gang activity.

In displaying the effects of BLOS C2 capabilities in the city of Salinas, a scenario similar to that of the City Wide Directed Enforcement operation will be used to analyze the potential benefits. This scenario serves to accurately represent SPD's operational state when local resources are exhausted. This can be due to either a large-scale cooperative effort such as the directed enforcement operation, or from an unforeseen disaster requiring outside assistance. As of yet, video sourced by the CCTV is only accessible by the watch commander who is occupied with a number of responsibilities. This causes the CCTVs to act as only deterrents, failing to process the information being captured by the five distributed cameras. Additionally, the MCV is virtually useless at the moment, lacking the computing and communication equipment to actively participate in command and control of an incident. As for the department's current interoperability efforts, the

[80] "City Wide Directed Enforcement Press Release," *Salinas Police Department* (Aug. 02, 2013): http://news.salinaspd.com/index.cfm/City_Wide_Directed_Enforcement_5640.htm#. UgtfoOChD0d (accessed Aug. 05, 2013).

[81] Ibid.

[82] Ibid.

200 P25 broadband radios procured via federal grants will contribute to NPSBN compliance and will provide the framework for BLOS C2 development. However, until NPSBN is fully deployed and these types of radios are issued nationwide, it will be difficult to seamlessly support cross-agency police/relief efforts. Figure 15 displays the current framework just described, showing how the architecture is enough to conduct day-to-day police work. Although this indicates that SPD is not fully utilizing department assets, BLOS C2 implementation could help integrate these components into the broad policing and response strategy.

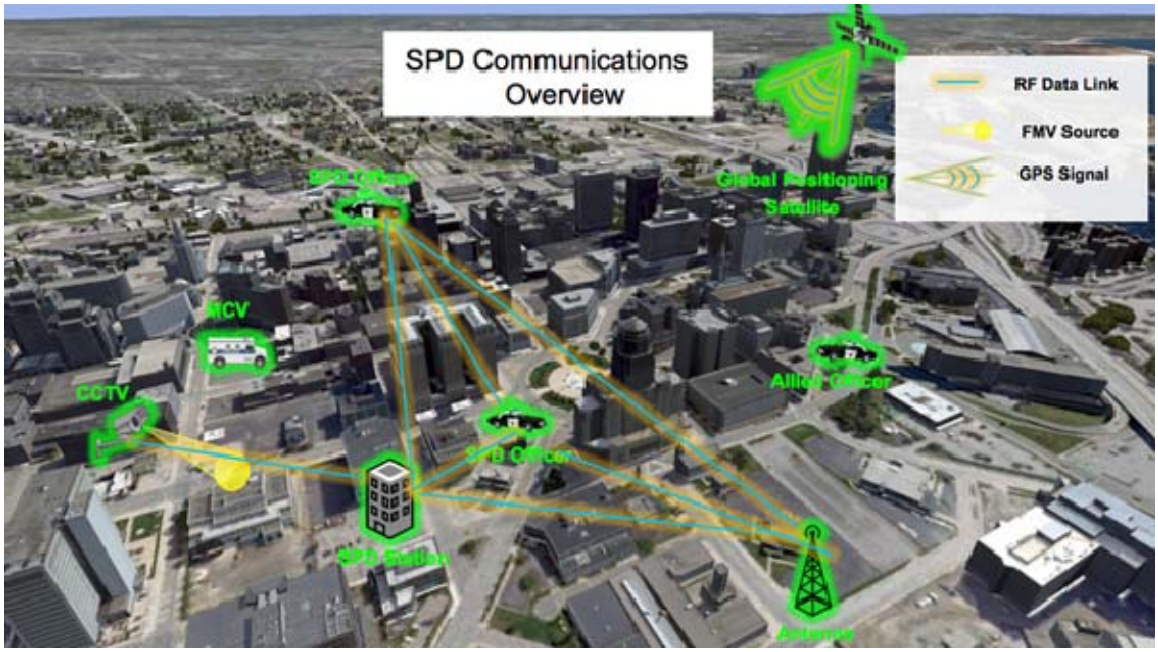

Figure 15. Existing SPD Communications Framework Overview.

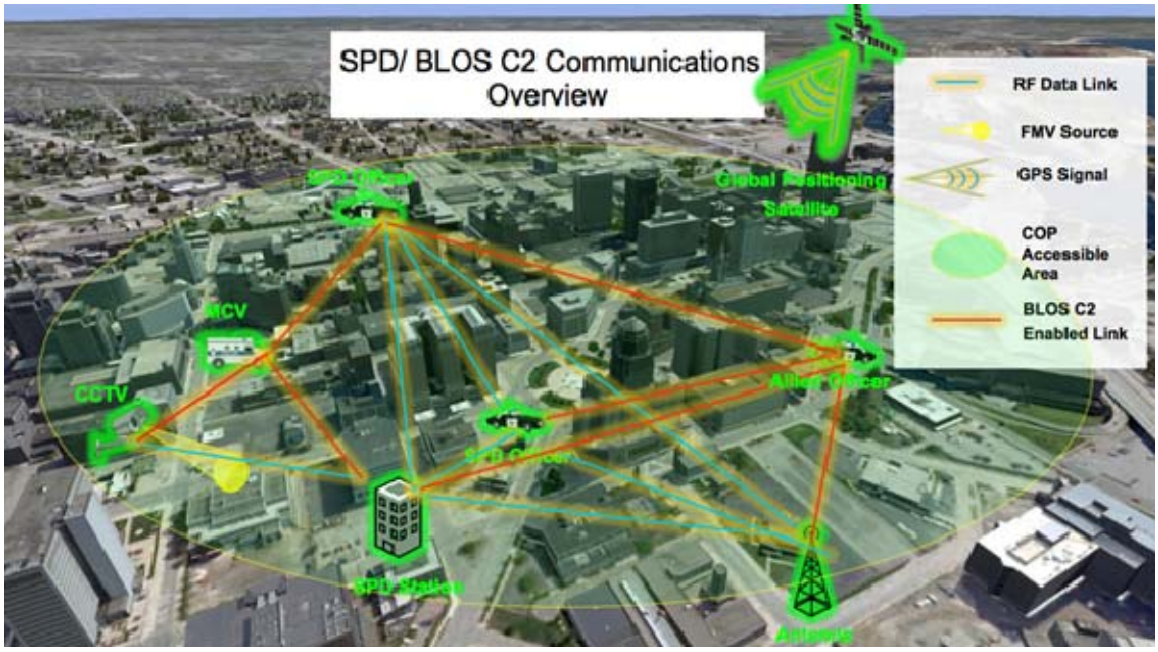

Figure 16. SPD Communications Framework with BLOS C2 Integration.

SPD's limited personnel resources make it imperative that asset control be carried out in day-to-day and emergency operations. SPD is another example of how a Common Operational Picture (COP) can help ensure personnel safety as well as the situational awareness (SA) of an environment. Up until SPD received the P25 radios, police officers were expected to verbally communicate their positions when dismounting from their patrol vehicles. This puts the officer in a vulnerable situation given the variety of ways in which an officer is incapable of operating his/her radio. The P25 radios recently acquired are all GPS enabled, providing real-time location data of every officer's whereabouts. These radios are also interoperable and software defined, meaning upgrades are performed by updating software rather than replacing the device altogether. Between the interoperability of the P25 radios and the NPSBN, additional assets from outside organizations have the capability to offer assistance without coming across frequency issues that could terminate communication links. The positioning data provided by these radios is also valuable for COP development, allowing watch commanders to monitor officer dismounts as well as manage assets during major incidents. With the COP distributed across the network, officers and allied partners can receive information regarding the whereabouts of suspected criminals, updated perimeter information, as well

as other data map layers that could give officers the upper hand. Figure 16 demonstrates this point, showing the possibility of sustaining a COP where one was not available in Figure 15 in the current SPD framework. Another big difference between the existing framework and the BLOS C2 enabled architecture is the distribution of CCTV video. Video multicasting can make CCTV cameras more than mere deterrents, allowing network users the opportunity to open video streams and monitor activities remotely. Lastly, by upgrading the MCV with BLOS C2 systems, the vehicle could be deployed during incidents such as disasters where close communications monitoring may be required due to network saturation. This would add to SPD's available incident response capabilities, while providing another layer of command and control.

All three case studies presented different scenarios in which BLOS C2 could leverage existing efforts to enhance disaster response and recovery capabilities. Each agency is at a different stage of development, all requiring some level of action in order to take full advantage of BLOS C2 and the coming nationwide emergency responder communications initiative. With these case studies in mind, in the next chapter, I suggest policy recommendations that will have the most impact on improving disaster response and recovery at each level of government.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. RECOMMENDATIONS FOR BLOS C2 IMPLEMENTATION AND INTEGRATION

Upon my initial assessment of existing DHS-led interoperability initiatives aimed at improving disaster response and recovery, the amount of emphasis placed on updating communications infrastructure was unclear. However, after learning about the progress that DHS has made through the NPSBN program, it is evident that providing an interoperable network to support disaster efforts is a high priority. The NPSBN is focused on providing a secure, reliable, and dedicated interoperable network for public service personnel to communicate in the event of an emergency. This initiative presents an opportunity for the BLOS C2 capability to provide network content and services to enhance the SA and C2 of an incident area. The implementation of this updated communications infrastructure requires the use of appropriate equipment and applications in order to establish network connectivity and participate in data exchanges. This implies the use of IP capable network devices and software applications intended specifically for the utilization of net-centric data and services. Additionally, the interoperability gained through the implementation of a nationwide broadband network creates an incentive to integrate DHS COPs with other public service mapping displays. Through the NPSBN, DHS has presented a progressive path toward interoperable communications and information sharing. Through the utilization of BLOS C2 network capabilities, DHS could build on the promising benefits that will be offered by the NPSBN. After evaluating the case study assessments that were offered in the previous chapter, the following recommendations will offer various possible courses of action for the implementation of the BLOS C2 capability. These recommendations are suggested in an effort to promote interoperability and information sharing across all levels of government, and ultimately improve disaster response and recovery efforts.

A. RECOMMENDATION #1—DHS SHOULD ENSURE THAT FUTURE ACQUISITIONS OF COMMUNICATION EQUIPMENT BE IP NETWORK CAPABLE

The first course of action that emerges from the findings of this thesis for DHS to secure a foundation for BLOS C2 integration is the assurance that future acquisitions of communication equipment be IP-network capable. As stated in the BLOS C2 overview in Chapter III, BLOS C2 promotes bi-directional data exchanges of different types (FMV, still imagery, SA data, and voice and text chat communications) through a specialized network architecture. Traditional radio frequencies are easily capable of supporting voice communications; however, higher bandwidth IP networks are required to pass larger data format types such as visual imagery, SA data, and chat communications. It is these high bandwidth data types that make the BLOS C2 capability advantageous in achieving mission objectives such as effective emergency response.

Although the NPSBN initiative is successfully emphasizing the application of P25 digital radios into the public safety community, this does not include the IP capability required to support the BLOS C2 net-centric capabilities. While the P25 radio standards ensure that public safety agencies are equipped with interoperable radio technology, instead of outdated equipment with limited availability of radio frequencies, it does not include the requirement to support wideband IP network connectivity. With that said, although P25 radios are interoperable, the utility is limited to voice communications. In order to tap into BLOS C2 hosted services and interface with software applications on compact PC devices, a network device with either a wireless or Ethernet interface is required to provide connectivity to the larger network. This enables both coordinating and ground-level response personnel the ability to subscribe and publish various types of information across the BLOS C2 network.

With DHS ensuring that future acquisitions of communication equipment be IP-network capable, public response personnel will be provided with the Internet connectivity required to access BLOS C2 and other network infrastructure. This thesis suggests going about this task in one of two ways. The first and most cost-effective option is through the procurement of P25 radios with IP capability (P25IP). These radios

combine industry standard IP-network technology and traditional digital radios to deliver a single solution that is capable of supporting multiple data exchange formats. This type of system would allow public service personnel the ability to connect devices directly to their radio units when in need of network accessibility. Not only does this all-in-one solution increase network reliability by minimizing the amount of potential points of failure on a network, it also minimizes the amount of equipment that personnel need to take with them when responding to an emergency. Additionally, top commercial communications vendors such as Harris, Cisco, and Raytheon offer variants of this radio system. The second option for providing Internet connectivity to personnel is through the acquisition of commercial cellular mobile broadband devices. These systems can come in both standalone "hotspot" forms, as well as built-in solutions that are integrated with portable PCs. This solution requires the purchase of an additional piece of communications equipment and data plans, resulting in higher costs. With the addition of this equipment, the most realistic method of issuing/installing these devices is by outfitting response vehicles with the technology rather than having personnel carry them. Under these circumstances, users would be required to connect to these vehicle-based devices over a wireless or wired Ethernet connection in order to upload or access data residing on the network. This circumstance can imply limited access and functionality, and also increases the amount of steps required to achieve network connectivity that can result in a weakened network signal. Although this option is not as convenient as the first, it is still a viable solution for providing network access to ground assets. All major cellular network providers offer variants of this solution as well, providing options for optimal cellular coverage.

In order to accomplish either of these network-providing options, it is recommended that DHS emphasize the importance of IP-compatible systems in order to drive the future procurement of capable communications equipment. One way that this can be approached is through the promotion of network data exchange capabilities such as BLOS C2. Through the identification of capability gaps that exist in current emergency response strategy, BLOS C2 could potentially provide solutions that create incentives for the procurement of IP-capable communications technology. More

importantly, this recommendation is essential to providing the fundamental network connectivity needed to access the BLOS C2 services and applications covered in the next section.

B. RECOMMENDATION #2—CREATE A DHS-SPONSORED, NATIONWIDE, STANDARDIZED SOFTWARE SUITE TO UTILIZE BLOS C2 NETWORK CAPABILITIES

The second recommendation for DHS to consider is a nationwide, standardized software suite for emergency responders. Once the NPSBN infrastructure is deployed and agencies have transitioned toward P25 digital IP-enabled radio equipment, emergency responders will have the interoperability means to access useful data being generated at multiple locations within an incident area. In order to utilize this data through the various BLOS C2 services, emergency responders must have a computer system with appropriate software applications to process and display the information. The BLOS C2 program addresses this with the software suite displayed in Figures 7 and 8, and the Special Operations community is equipped with battlefield air operations (BAO) kits to accomplish the same goal.[83] Like the BLOS C2 software suite, the BAO kit applications allow the warfighter to send intelligence data from machine to machine through network properties. Fred Pushies, author of *U.S. Air Force Special Ops*, describes the importance of these applications by stating that, "while technology is a wonderful thing, it must be remembered that to be of any tactical value it must be placed in the hand of the battlefield airman."[84] This applies to the emergency responder as well. With vital sensor and SA data being generated during an emergency, it is important to package the information in a way that can reach the ground user directly in order to aid an effective and timely response.

Like the Special Operations community, DHS would be well served by creating a standardized software suite that could be adopted nationwide by public service agencies in order to achieve optimal benefits from the BLOS C2 services. This software suite would run on compact machines such as laptops or tablet PCs as part of public safety-

[83] Fred Pushies (2000), U.S. Air Force Special Ops, St. Paul: Zenith Press, Print, 117.

[84] Ibid.

deployable equipment that could either be vehicle or personally mounted. In doing so, DHS should focus on the major use cases that would aid emergency response efforts the most. Once these use cases have been identified, market research of various software applications could be conducted to cater to the specific needs of the public service community. The major use cases that should be emphasized would be: 1) Situational Awareness (SA) development; 2) chat and voice communications; and 3) still imagery and Full Motion Video (FMV) distribution and viewing.

One of the main benefits gained from the BLOS C2 capability is the enhanced SA picture derived from the various position and targeting technologies that are deployed with ground personnel. Providing a solution for this use case incorporates the generation, distribution, and display of the data within a COP for users at the coordinative and ground levels. Enterprise data sources such as emergency dispatch records could contribute to the improved environmental awareness of an incident area assuming a network connection is made to the database. In addition to the utilization of enterprise SA data, information being generated at the local level needs to be accessible to network users. Examples of local SA data are precise position and location information (PPLI) and sensor points of interest (SPoI). These two data sources aid in the control of assets and personnel, while also allowing users the ability to create spot reports on a map of locations that may require special attention. The software applications needed to support these capabilities should address mapping, targeting, tracking, and message translating. The Department of Defense (DoD) and Special Operations community rely on Cursor on Target (CoT) software to perform most of these tasks; however, DHS may discover other commercial products by way of market research.

Another benefit to the BLOS C2 capability is the ability to participate in voice and text communications through a computer. This use case requires the ability to take part in chat room/group discussions while maintaining audio communications as well. Text chatting introduces the ability to focus on specific users by creating focused chat rooms, while maintaining the history of conversations for after-action review or general reference during a disaster. Additionally, it is possible to carry out voice communications over an Internet network through a method known as Voice over Internet Protocol

(VoIP). VoIP is the process of taking analog audio signals and converting them into digital data, making it possible to transmit them over the Internet. Like a text chat room, the VoIP method allows administrators the ability to create broad and/or focused groups to participate in, acting like a traditional channel on a radio frequency. With a capable radio providing IP-network connectivity, VoIP allows the operator to maintain traditional voice communications while using the same link to pass other forms of useful data such as SA data and FMV. The software applications needed to support these capabilities should address peer-to-peer chatting (in order to avoid a host server) and VoIP call management. There are a variety of proprietary and open source clients on the market that can perform both of these tasks.

Lastly, still imagery and FMV generation and distribution is a use case that could be utilized by the BLOS C2 capability. In order to address this use case, software must be capable of viewing, storing, and sending both still images and real-time FMV. Visual aids offer a perspective that is irreplaceable when attempting to provide personnel with information that is difficult to explain with words. Still imagery can accomplish this while taking up only a moderate amount of network bandwidth. With more network availability and a live-streaming video source, FMV can offer accurate representation of environmental conditions to public safety personnel through the process of multicasting described in Chapter III. With the use of cameras in existing response practices, the ability to package and send visual data to network participants could offer substantial benefits. With the proper software, public service personnel participating in the BLOS C2 network could share and display mission-critical still imagery and FMV in order to effectively gauge response tactics. The software applications needed to support these capabilities should address still imagery and FMV: viewing, annotation, multicasting, and distribution. Storage and management of this data can be conducted by BLOS C2 services and standard Windows applications, along with popular open source video-playing software, can handle most of the other tasks listed as well.

With the development of a standardized software suite sponsored by DHS, public safety agencies can be prepared to actively participate in emergency response efforts that offer BLOS C2 network capabilities. The ability to implement the software suite on a

national level will largely rely on the effectiveness and accessibility of the product. Agencies must have a good reason to put the effort into learning the new software, as well as have an easy method of accessing the applications. With the proper research and organization of this recommended course of action, DHS could improve existing disaster response and recovery tactics.

C. RECOMMENDATION #3—INTEGRATE EXISTING DHS COP EFFORTS WITH OTHER FEDERAL, STATE, AND LOCAL COP INITIATIVES

The implementation of the second recommendation offers a method for BLOS C2 users to actively engage in a COP. As described in Chapter III, a COP provides users with a mutual perspective of an incident area by tying in all of the available data resources that have an established connection to the shared network. The result is a useful tool that complements traditional voice communications. Although the COP is intended to be "common," as suggested in its name, agencies across DHS, such as the USCG, have developed standalone COPs that do not promote integration across the department as a whole. This issue presents inefficiencies in attempting to provide an interoperable solution for emergency response and recovery command and control. With that said, although the addition of a BLOS C2 COP could improve response strategies, it is recommended that DHS integrate existing agency COP efforts with other federal, state, and local COP initiatives. This recommendation would not only improve interagency information sharing, a major takeaway from the *9/11 Commission Report*, it would also expand on the amount of information available that could support various public safety missions.

In an effort to create synergies among its 22 agencies, DHS Chief Information Officer Richard Spires publicly expressed the desire to integrate various department programs including COPs.[85] Agencies under DHS that have relied on COP technology include the USCG, FEMA, National Protection and Programs Directorate, and Customs and Border Protection (CBP), to name a few. With more than 20 COPs spread across

[85] Alice Lipowicz, "DHS agencies starting to integrate missions, CIO says," *FCW* (May 11, 2012): http://fcw.com/articles/2012/05/11/dhs-integration.aspx (accessed Aug. 15, 2013).

DHS, Spires said, "We all have COPs, but no real integration."[86] COP technology is currently being utilized in FEMAs main emergency operations center, displaying information such as weather conditions, positioning of FEMA personnel and assets, main transportation routes, and areas of damaged structures or roads and location of shelters on a map display.[87] The technology also provides CBP with border security information, and the USCG with maritime conditions to assist in carrying out mission objectives. DHS has realized that the integration of the various COPs across the department could offer shared benefits in carrying out national security; already, DHS has started to merge these efforts by integrating some of the 117 identity-screening programs that are used across the department.[88] Although this is a positive move toward department-wide integration, it is recommended that efforts be made to extend the collaboration with other federal, state, and local agencies that either already have, or can benefit from COP initiatives.

In order to share COP-relevant information across various agencies at all levels of government, a standardized format for different types of data must be created and mandated to create seamless data exchanges. This would aid in the integration of existing DHS COP initiatives with similar mapping efforts, as suggested earlier. Contributing to the accomplishment of this task is the Global Justice XML Data Model (GJXDM), first introduced in 2003. This effort sought to solve challenges involving information sharing through the creation of well-defined data elements that would provide a model for data interoperability.[89] In 2005, this effort became known as the National Information Exchange Model (NIEM), and was initiated by DHS and the U.S. Department of Justice (DOJ), successfully uniting major stakeholders from all levels of government toward a common model for information sharing.[90] The NIEM website states that, "all 50 states as

[86] Alice Lipowicz, "DHS agencies starting to integrate missions, CIO says," *FCW* (May 11, 2012): http://fcw.com/articles/2012/05/11/dhs-integration.aspx (accessed Aug. 15, 2013).

[87] Ibid.

[88] Ibid.

[89] Van Hitch, "History of the National Information Exchange Model," *NIEM website:* https://www.niem.gov/aboutniem/Pages/history.aspx (accessed Aug. 17, 2013).

[90] Ibid.

well as 19 federal agencies are committed to using NIEM at varying levels of maturity," which provides the user-base and platform for integrating COP data.[91]

With the evolving development and use of NIEM, a medium has been provided to guide COP integration across federal, state, and local agencies. However, unless organizations are mandated to comply with the NIEM data-sharing model, interoperability gaps will continue to exist within the public service community. Without this step being taken, relevant data will be prevented from being accessed by partnering agencies that may find the information useful in carrying out critical mission objectives. This includes the vast amount of COP data that is exclusively available to individual agencies. For this reason, my findings in this thesis suggest that DHS mandate the compliance of the NIEM data-sharing model for public service agencies at all levels of government. Once this is accomplished, existing DHS COP efforts could more easily integrate with other federal, state, and local COP initiatives, as well as a BLOS C2 COP.

[91] Van Hitch, "History of the National Information Exchange Model," *NIEM website:* https://www.niem.gov/aboutniem/Pages/history.aspx (accessed Aug. 17, 2013).

THIS PAGE INTENTIONALLY LEFT BLANK

V. FUTURE RESEARCH RECOMMENDATIONS AND CONCLUSION

A. FUTURE RESEARCH RECOMMENDATIONS

The findings of this thesis highlight some useful directions for future research. Based on the ongoing efforts conducted by DHS to implement the NPSBN and improve interoperability, as well as the recommendations made in the previous chapter, the following topics are recommended for future research:

- The continued evolution of the NPSBN.
- Evaluation of the government-wide implementation of the NPSBN.
- The adaptability of NGEN P25 radios by the public safety community.
- The continued DHS efforts to integrate department and other government COP efforts.
- DHS' prioritization of emphasizing IP-capable communications equipment to support the exchange of multiple data formats.
- A DHS-sponsored creation of a standardized software suite aimed at improving COP interaction and data exchanges.

These research topics address implementations that could improve disaster response and recovery aside from BLOS C2 specific involvement. BLOS C2 could address some of these topics; however, the topics listed above provide the best platforms for further research due to content availability.

B. CONCLUSION

This thesis introduced the BLOS C2 capability as a method of improving disaster response and recovery by enhancing situational awareness (SA) as well as command and control (C2). Inspired by historical shortcomings that resulted in the devastating loss of American lives, the BLOS C2 capability promotes seamless communication and data sharing by means of sensor data and a truly common operational picture (COP). This capability has proven to be a useful resource for the U.S. military on the battlefield,

utilizing various ISR sensor data to improve battlespace coordination and fulfill critical military objectives. The ability to improve SA and C2 is a valuable capability for our nation's domestic missions as well, especially in disaster scenarios that threaten homeland security. Using the proven model that has improved mission effectiveness for the U.S. military, this thesis used the Department of Homeland Security and other levels of government involved in emergency response as case studies for analyzing the BLOS C2 capability in an effort to fill gaps in interoperability and information sharing. Fortunately, at the federal level, DHS has been focusing on addressing these very capability gaps ever since the release of the *9/11 Commission Report*, and increasingly so after Hurricane Katrina. Feeding off of DHS' existing efforts, this thesis developed a series of case studies to analyze and assess DHS interoperability and information-sharing efforts at the federal, state, and local levels of government. The USCG, CAL FIRE, and SPD were used to conclude whether or not the BLOS C2 capability could improve disaster response and recovery efforts. In each circumstance, the implementation of BLOS C2 capabilities displayed a potential to improve general mission fulfillment as well as emergency response tactics in particular. While these agencies displayed varying degrees of interoperability and information-sharing abilities, this thesis drew on all of the case study assessments to provide recommendations aimed at assisting the implementation of the BLOS C2 capability. These recommendations were made to assist DHS in closing interoperability and information-sharing gaps, and ultimately improving disaster response and recovery efforts.

In the process of determining where the most improvements needed to be made across the various levels of government, this thesis revealed that DHS has addressed most of the major problem areas through the Nationwide Public Service Broadband Network (NPSBN) initiative. Focused on providing a dedicated section of radio spectrum for public safety use, the NPSBN is actively establishing an interoperable communications infrastructure in order to ensure network availability during emergency situations. The current developmental phase of the NPSBN presents a unique opportunity to introduce technologies that could further contribute to and benefit from the initiative such as BLOS C2. With the evolution of this public safety network, solutions for managing and

producing network content become increasingly relevant. The integrative Common Operating Picture (COP) technology that the BLOS C2 introduces, along with the ability to send and view useful sensor data residing on a network, make BLOS C2 a valuable asset in improving response efforts at the coordinative and ground level.

In continuing the effort to promote interoperability and information sharing across the various public service agencies, DHS will face challenges in ensuring that communication standards are carried out nationwide. In order to cover all aspects of network interoperability, DHS must take into consideration the services, capabilities, and applications that will reside on NPSBN. By considering the recommendations laid out in the previous chapter of this thesis, and implementing the BLOS C2 capability, DHS can provide the public service community with network content that could enhance SA and C2, improving response and recovery efforts in the event of a disaster.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

107th Congress. "An Act to establish the Department of Homeland Security, and for other purposes." Public Law 107–296-NOV. 25, 2002. http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf.

"About the Office of Emergency Communications." U.S. Department of Homeland Security. http://www.dhs.gov/about-office-emergency-communications.

AccuWeather. "Intense Storms Called a "'Derecho'" Slam 700 Miles of the U.S.." 2012. http://www.accuweather.com/en/weather-news/deadly-super-derecho-strikes-m/67383. Web.

Bercovici, Martin. *FCC Narrowbanding Mandate: A Public Safety Guide for Compliance.* Fairfax, VA: International Association of Fire Chiefs, 2006.

Bimfort, Martin. "A Definition of Intelligence." *Central Intelligence Agency, Center for the Study of Intelligence.* 2007. https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol2no4/html/v02i4a08p_0001.htm.

"C3CEN Projects." *United States Coast Guard.* 2013. http://www.uscg.mil/hq/c3cen/projects.asp.

California Department of Forestry and Fire Protection. "CAL FIRE at a Glance." Dec. 2009. http://www.fire.ca.gov/communications/downloads/fact_sheets/Glance.pdf.

———. "CAL FIRE Mobile Communications Center (MCC)." April 2011. http://www.fire.ca.gov/communications/downloads/fact_sheets/MCC.pdf.

———. "2012 Strategic Plan." 2012. 15. http://www.fire.ca.gov/about/downloads/Strategic_Plan/StrategicPlan_SinglePages.pdf.

———. "What is CAL FIRE?" www.fire.ca.gov/communications/downloads/.../WhatisCALFIRE.pdf.

"City Wide Directed Enforcement Press Release." *Salinas Police Department.* Aug. 02, 2013. http://news.salinaspd.com/index.cfm/City_Wide_Directed_Enforcement_5640.htm#. UgtfoOChD0d.

"Crime rates for Salinas, CA." *Neighborhood Scout*. 2013. http://www.neighborhoodscout.com/ca/salinas/crime/#data.

Dubay, Jerome. “Implementing Joint Battlespace Awareness IST Integration Capability Architecture: A Crime-Reduction Strategy in Salinas, California.” (Master’s thesis, Naval Postgraduate School, June 2011).

“Emergency Communications Preparedness Center.” *U.S. Department of Homeland Security*. http://www.dhs.gov/emergency-communications-preparedness-center.

“Employment with the Salinas Police Department.” *Salinas Police Department*. 2013. http://www.salinaspd.com/employment-general.

Essid, Chris. “Nationwide Public Safety Broadband Network.” *U.S. Department of Homeland Security.* June 2012. http://www.dhs.gov/sites/default/files/publications/Fact%20Sheet_Nationwide%20Public%20Safety%20Broadband%20Network.pdf. (accessed Apr. 07, 2013). Web.

Executive Office of the President. “Executive Order -- Assignment of National Security and Emergency Preparedness Communications Functions.” July 2012. http://www.whitehouse.gov/the-press-office/2012/07/06/executive-order-assignment-national-security-and-emergency-preparedness-.

———. “Federal Response to Hurricane Katrina,” Feb. 2006. http://www.library.stmarytx.edu/acadlib/edocs/katrinawh.pdf.

Federal Communications Commission. “700 MHz.” http://www.fcc.gov/topic/700-mhz.

Fetherolf, L., “Message from Chief Louis Fetherolf.” *Salinas Police Department Report to the Community,* July 1, 2010. http://news.salinaspd.com/index.cfm/Message_from_Salinas_Police_Chief_Louis_Fetherolf_4358.htm#.UjNygRZ41QU.

"GIS for Disaster Response." *ESRI.* http://www.esriro.ro/services/disaster-response/disaster-relief.html (accessed May 14, 2013). Web.

Glor, Jeff. “Drone use in the U.S. raises privacy concerns.” *CBS News*. 2012. http://www.cbsnews.com/8301–505263_162–57409759/drone-use-in-the-u.s-raises-privacy-concerns/.

Griffin, P. F., and White, L., “Lettuce Industry of the Salinas Valley.” *The Scientific Monthly.* 81.2. 1955, 77. http://ccwg.mlml.calstate.edu/sites/default/files/projects/gabilanHEP/griffinwhite_1955_lettuce_industry_salinasvalley.pdf.

Heide, Erik A. D. “Disaster Response: Principles of Preparation and Coordination.” *C.V. Mosby Company*. 1989. 101. http://www.coe-dmha.org/Media/Disaster_Response_Principals.pdf

Hitch, V. “History of the National Information Exchange Model.” NIEM website. https://www.niem.gov/aboutniem/Pages/history.aspx.

Husick, Chuck. “VHF Radios.” *Boat U.S.* Sept. 2009. http://www.boatus.com/husick/c_vhf.asp.

Lipowicz, Alice. “DHS agencies starting to integrate missions, CIO says.” *FCW*. May 11, 2012. http://fcw.com/articles/2012/05/11/dhs-integration.aspx.

Lolich, Richard. “Marine Transportation System (MTS).” *U.S. Department of Transportation, Maritime Administration.* http://www.marad.dot.gov/ports_landing_page/marine_transportation_system/MTS.htm.

Lungren, Dan. “Subcommittee Hearing: The EMP Threat: Examining the Consequences.” *U.S. House of Representatives Committee On Homeland Security.* Sept. 12, 2012. http://homeland.house.gov/hearing/subcommittee-hearing-emp-threat-examining-consequences.

Magnier, M., and Sharma, S. “Terror Attacks Ravage Mumbai.” *Los Angeles Times.* Nov. 27, 2008. http://articles.latimes.com/2008/nov/27/world/fg-mumbai27.

“Maritime Communications.” *United States Coast Guard, Navigation Center* .2012. http://www.navcen.uscg.gov/?pageName=maritimeTelecomms.

Mendoza, Georgina. “Salinas Comprehensive Strategy for Community-wide Violence Reduction.” *City of Salinas.* http://www.ci.salinas.ca.us/pdf/SalinasSWP.pdf.

Miller, Greg. “Brennan speech is first Obama acknowledgement of use of armed drones.” *The Washington Post.* 2012. http://www.washingtonpost.com/world/national-security/brennan-speech-is-first-obama-acknowledgement-of-use-of-armed-drones/2012/04/30/gIQAq7B4rT_story.html.

National Commission on Terrorist Attacks upon the United States (2004). *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*. Washington, DC.

“National Emergency Communications Plan (NECP) Goals.” *U.S. Department of Homeland Security*. http://www.dhs.gov/national-emergency-communications-plan-necp-goals.

“The Nationwide Public Safety Broadband Network: First Steps.” *U.S. Department of Homeland Security.* June 2012. http://www.dhs.gov/sites/default/files/publications/Case%20Study_Broadband%20FirstSteps.pdf.

"Nationwide Public Safety Broadband Network (NPSBN)." *Illinois First Net.* http://www.illinois.gov/firstnet/NPSBN/Pages/default.aspx.

Norris, Guy. " Real-Time Intelligence, Surveillance & Reconnaissance (ISR) Data Sharing Technology for the "Af/Pak" Theatre," *American At War.* July 2009. http://afpakwar.com/blog/archives/1316.

"OEC Architecture and Advanced Technology Branch." *U.S. Department of Homeland Security*. http://www.dhs.gov/oec-architecture-and-advanced-technology-branch.

"OEC Communications Portfolio Management Branch." *U.S. Department of Homeland Security*. http://www.dhs.gov/oec-communications-portfolio-management-branch.

"OEC Policy and Planning Branch." *U.S. Department of Homeland Security*. http://www.dhs.gov/oec-policy-and-planning-branch.

"OEC Regional Coordination Program." *U.S. Department of Homeland* Security. http://www.dhs.gov/oec-regional-coordination-program.

"Office of Emergency Communications Technical Assistance Program." *U.S. Department of Homeland Security*. http://www.dhs.gov/office-emergency-communications-technical-assistance-program.

"Ports, Waterways, and Coastal Security (PWCS)." *United States Coast Guard* .2013. http://www.uscg.mil/hq/cg5/cg532/pwcs.asp.

"Public Safety Technical Assistance Tools." *Interoperable Communications Technical Assistance Program*. http://www.publicsafetytools.info/start_index_v2.php.

Pushies, Fred. *U.S. Air Force Special Ops*. St. Paul: Zenith Press, 2000.

Rayburn, A. "Written testimony of U.S. Coast Guard Deputy Commandant for Operations Vice Admiral Peter Neffenger for a House Committee on Transportation and Infrastructure, Subcommittee on Coast Guard and Maritime Transportation hearing titled 'A Review of Federal Maritime Domain Awareness Programs.'" *U.S. Department of Homeland Security.* .July 2012. http://www.dhs.gov/news/2012/07/03/written-testimony-us-coast-guard-house-transportation-and-infrastructure.

Reynolds, Julia. "NPS system gives Salinas police field data in real time." *The Monterey Herald*, accessed Sept. 03 2012. http://www.montereyherald.com/local/ci_21440031/nps-creates-system-that-gives-salinas-police-field.

"SAFECOM Program." *U.S. Department of Homeland Security*. http://www.dhs.gov/safecom-program.

Samenow, Jason. “Derecho: Behind Washington, D.C.’s destructive thunderstorm outbreak.” June 29, 2012. http://www.washingtonpost.com/blogs/capital-weather-gang/post/derecho-behind-washington-dcs-destructive-thunderstorm-outbreak-june-29–2012/2012/06/30/gJQA22O7DW_blog.html.

Sandman, Peter. “Dilemmas in Emergency Communication Policy.” *Emergency Risk Communication, Center for Disease Control and Prevention*. 2003. www.psandman.com/articles/dilemmas.pdf.

Shapiro, Ari. “Are Drones Obama’s Legacy In War On Terrorism?” *NPR*. June 2012. http://www.npr.org/2012/06/20/155389081/are-drones-obamas-legacy-in-war-on-terrorism.

“Statewide Interoperability Coordinators.” *U.S. Department of Homeland Security*. http://www.dhs.gov/statewide-interoperability-coordinators.

“Statewide Interoperability Plans.” *U.S. Department of Homeland Security*. http://www.dhs.gov/statewide-communication-interoperability-plans.

Stempfley, Roberta. “Written testimony of NPPD for a House Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies hearing titled ‘Resilient Communications: Current Challenges and Future Advancements.’” *U.S. Department of Homeland Security.* Sept. 2012. http://www.dhs.gov/news/2012/09/12/written-testimony-nppd-house-homeland-security-subcommittee-cybersecurity-0.

“TDC Security Alert: Maritime Aspects of Mumbai Terror Attacks.” *The Maritime Executive.* Dec. 04, 2008. http://www.maritime-executive.com/article/tdc-security-alert-maritime-aspects-mumbai-terror-attacks/.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California